



SuperStack® 3

Firewall

User Guide

SuperStack 3 Firewall 3CR16110-95
SuperStack 3 Firewall Web Site Filter 3C16111

<http://www.3com.com/>

Part No. DUA1611-0AAA03
Published September 2002



3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

Copyright © 2002, 3Com Technologies. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Technologies.

3Com Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies to provide notification of such revision or change.

3Com Technologies provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo and SuperStack are registered trademarks of 3Com Corporation. CoreBuilder is a trademark of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

ENCRYPTION

This product contains as standard 56 bit encryption and may require US and/or local Government authorization prior to export or import to another country

CONTENTS

ABOUT THIS GUIDE

How to Use This Guide	14
Conventions	14
Terminology	15
Feedback about this User Guide	17
Registration	18

I GETTING STARTED

1 INTRODUCTION

What to Read if You are in a Hurry	21
What is the SuperStack 3 Firewall?	22
Firewall and 3Com Network Supervisor	23
Firewall Features	25
Firewall Security	25
Web URL Filtering	26
High Availability	27
Logs and Alerts	27
User Remote Access (from the Internet)	28
Automatic IP Address Sharing and Configuration	28
Introduction to Virtual Private Networking (VPN)	28
Virtual Private Networking	28

2 INSTALLING THE HARDWARE

Before You Start	31
Positioning the Firewall	32
Rack Mounting the Units	32
Securing the Firewall with the Rubber Feet	33
Firewall Front Panel	34

Firewall Rear Panel	35
Redundant Power System (RPS)	36
Attaching the Firewall to the Network	37

3 QUICK SETUP FOR THE FIREWALL

Introduction	41
Setting up a Management Station	42
Configuring Basic Settings	43
Setting the Password	43
Setting the Time Zone	44
Configuring WAN Settings	45
Automatic WAN Settings	45
Manual WAN Settings	45
Using a Single Static IP Address	47
Using Multiple Static IP Addresses	48
Using an IP Address provided by a PPPoE Server	50
Using a Static IP address provided by a DHCP Server	50
Configuring LAN Settings	51
Automatic LAN Settings	51
Entering information about your LAN	51
Configuring the DHCP Server	52
Confirming Firewall Settings	53

II CONFIGURING THE FIREWALL

4 BASIC SETTINGS OF THE FIREWALL

Examining the Unit Status	59
Configuring the Administrator	60
Administrator login name	60
Change the Administrator Password	60
Administrator Inactivity Timeout	60
Administrator and User Login Failure Handling	61
Setting the Time	61
Set Time and Date	62
NTP Configuration	62
Changing the Basic Network Settings	63

Setting the Network Addressing Mode	63
Specifying the LAN Settings	64
Specifying the WAN/DMZ Settings	66
Specifying the DNS Settings	67
Specifying DMZ Addresses	67
Setting up the DHCP Server	69
Global Options	69
Dynamic Ranges	70
Static Entries	71
Setting up DHCP over VPN	71
Configuring a Central Gateway	72
Configuring a Remote Gateway	73
Viewing the DHCP Server Status	75
Using the Network Diagnostic Tools	76
Choosing a Diagnostic Tool	76

5 SETTING UP WEB FILTERING

Configuring the Filtering Options	79
Content Filtering	80
Restricting the Web Features Available	81
Using Trusted Domains	82
Changing the Message to display when a site is blocked	82
Configuring the URL List	83
Checking the Web Filter Status	83
Updating the Web Filter	83
Setting Actions if no Filter List is Loaded	84
Specifying the Categories to Filter	85
Customizing the 3Com Web Filter	85
Setting up Trusted and Forbidden Domains	86
Using Keyword Filtering	87
Specifying When Filtering Applies	87
Setting Blocking Options	88
Filtering by User Consent	88
Configuring User Consent Settings	89
Mandatory Filtered IP Addresses	90
Configuring the Firewall for use with N2H2	91
N2H2 Status	92

Settings	92
URL Cache	92
Configuring the Firewall for use with Websense Enterprise	93
Websense Server Status	93
Settings	93
URL Cache	94

6 USING THE FIREWALL LOG AND TOOLS OPTIONS

Logs and Alerts	95
Viewing the Log	96
Changing Log and Alert Settings	98
Sending the Log	98
Changing the Log Automation Settings	100
Selecting the Categories to Log	101
Alert Categories	102
Generating Reports	103
Collecting Report Data	103
Viewing Report Data	104
Restarting the Firewall	105
Managing the Firewall Configuration File	106
Importing the Settings File	107
Exporting the Settings File	108
Restoring Factory Default Settings	108
Using the Installation Wizard to reconfigure the Firewall	108
Upgrading the Firewall Firmware	109

7 SETTING A POLICY

Changing Policy Services	113
Amending Network Policy Rules	114
Changing NetBIOS Broadcast Settings	115
Enabling Detection Prevention	116
Setting the Network Connection Inactivity Timeout	116
Adding and Deleting Services	116
Adding and Editing Policy Rules	119
Viewing Network Policy Rules	119
Adding a New Rule	121
Restoring Rules to Defaults	123

Configuring Users	123
Global User Settings	124
Setting User Privileges	124
Establishing an Authenticated Session	127
Configuring the Firewall to use a RADIUS Server	127
Configuring the Radius Global Settings	128
Specifying the RADIUS Servers	128
Configuring RADIUS User Privileges	129
Configuring the RADIUS Client Test	130
Configuring Management	130
Configuring SNMP Management	131
Setting the Management Method	133
Selecting Remote Management	133
HTTPS Management	134
Using the Firewall with the NBX Business Telephone System	135

8 ADVANCED SETTINGS

Automatic Proxy/Webcache Forwarding	137
Deploying the SuperStack 3 Webcache as a Proxy of the Firewall	139
Specifying Intranet Settings	140
Installing the Firewall to Protect the Intranet	141
Configuring the Firewall to Protect the Intranet	141
Setting Up Static Routes	143
Setting up One-to-One NAT	145
Configuring the Ethernet Port Settings	147
Ethernet Settings	148
MTU Settings	148

9 CONFIGURING VIRTUAL PRIVATE NETWORK SERVICES

Editing VPN Summary Information	151
Changing the Global IPSec Settings	152
Configuring VPN Bandwidth Management	153
Viewing the Current IPSec Security Associations	153
Configuring a VPN Security Association	154
Adding/Modifying IPSec Security Associations	154
Security Policy Settings for IKE using Pre-Shared Secret	155
Security Policy Settings for IKE Using 3rd Party Certificates	157

Security Policy Settings using Manual Key	157
Encryption Methods	159
Peer Certificate's ID	161
Use the SA as the default route for all Internet traffic	161
Destination network obtains IP addresses using DHCP through this SA	161
Setting the Destination Network for the VPN Tunnel	161
Advanced Settings for VPNs	162
Configuring the IRE VPN Client for use with the Firewall	166
Setting up the GroupVPN Security Association	166
Installing the IRE VPN Client Software	167
Configuring the IRE VPN Client	167
Setting up L2TP Clients	168
Using Third Party Digital Certificates	169
Overview	169
Third Party Digital Certificate Support	169
Configuring the Firewall for use with CA Certificates	170
Import Certificate	171
Viewing Certificate Details	171
Configuring the Firewall for use with Local Certificates	171
Current Certificates	172
Import Certificate with Private Key	173
Generate Certificate Signing Request	173
Importing a Signed Local Certificate	174
Configuring a VPN Security Association using IKE and a Third Party Certificate	175
Configuring the Firewall as an L2TP Server	176
General	176
L2TP Settings	176
L2TP Local IP Pool Settings	177
L2TP Active Sessions	177

10 CONFIGURING HIGH AVAILABILITY

Getting Started	179
Network Configuration for High Availability Pair	180
Configuring High Availability	181
Viewing the High Availability Status	181
Configuring High Availability on the Primary Firewall	182

Configuring High Availability on the Backup Firewall	183
Firmware Upgrades	183
Checking High Availability Status	183
High Availability Status Window	184
E-Mail Alerts Indicating Status Change	185
View Log	185
Forcing Transitions	186

III ADMINISTRATION AND TROUBLESHOOTING

11 ADMINISTRATION AND ADVANCED OPERATIONS

Introducing the Web Site Filter	189
Activating the Web Site Filter	192
Using Network Access Policy Rules	193
Understanding the Rule Hierarchy	194
Examples of Network Access Policies	195
Resetting the Firewall	198
Resetting the Firewall	199
Reloading the Firmware	199
Direct Cable Connection	200
Direct Connection Instructions	201

12 TROUBLESHOOTING

Introduction	203
Potential Problems and Solutions	203
Power LED Not Lit	203
Power LED Flashes Continuously	204
Power and Alert LED Lit Continuously	204
Link LED is Off	204
Ethernet Connection is Not Functioning	204
Cannot Access the Web interface	204
LAN Users Cannot Access the Internet	205
Firewall Does Not Save Changes	205
Duplicate IP Address Errors Are Occurring	205
Machines on the WAN Are Not Reachable	206
Troubleshooting the Firewall VPN Client	206

The IKE Negotiation on the VPN Client	206
Restarting the Firewall with Active VPN Tunnel	207
Export the VPN Client Security Policy File	207
Import the VPN Client Security Policy File	207
Uninstall the VPN Client	207
Frequently Asked Questions about PPPoE	208

IV FIREWALL AND NETWORKING CONCEPTS

13 TYPES OF ATTACK AND FIREWALL DEFENCES

Denial of Service Attacks	211
Ping of Death	211
Smurf Attack	211
SYN Flood Attack	212
Land Attack	212
Intrusion Attacks	212
External Access	212
Port Scanning	213
IP Spoofing	213
Trojan Horse Attacks	213

14 NETWORKING CONCEPTS

Introduction to TCP/IP	215
IP and TCP	215
IP Addressing	215
Network Address Translation (NAT)	218
Limitations of Using NAT	219
Dynamic Host Configuration Protocol (DHCP)	219
Port Numbers	220
Well Known Port Numbers	220
Registered Port Numbers	220
Private Port Numbers	220
Virtual Private Network Services	221
Introduction to Virtual Private Networks	221
VPN Applications	221
Basic VPN Terms and Concepts	223

IPSec Protocol	226
L2TP Protocol	227
Bandwidth Management	228
Why Use Bandwidth Management?	228
The Firewall and Bandwidth Management	229
How Does It Work?	229
Enabling Bandwidth Management	231
RADIUS Server Configuration	231
Steel Belted RADIUS from Funk Software	231
ACE Server from RSA	233
Internet Authentication Service on Microsoft Windows NT/2000 Server	233
RADIUS Attributes Dictionary	235

V APPENDICES

A SAFETY INFORMATION

Important Safety Information	239
Wichtige Sicherheitshinweise	240
Consignes Importantes de Sécurité	241

B TECHNICAL SPECIFICATIONS AND STANDARDS

C CABLE SPECIFICATIONS

Cable Specifications	245
Pinout Diagrams	245

D TECHNICAL SUPPORT

Online Technical Services	247
World Wide Web Site	247
3Com Knowledgebase Web Services	247
3Com FTP Site	248
Support from Your Network Supplier	248
Support from 3Com	249
Email Support	249

Telephone Support	249
Returning Products for Repair	251

INDEX

REGULATORY NOTICES

ABOUT THIS GUIDE

This guide describes the following products:

- SuperStack 3 Firewall 3CR16110-9x running v6.3 firmware
- SuperStack 3 Firewall Web Site Filter 3C16111

Introduction

This guide describes how to set up and maintain the SuperStack® 3 Firewall and how to install and use the SuperStack 3 Web Site Filter.

The Firewall acts as a secure barrier to protect a private LAN from hacker attacks from the Internet. It can also be used to control the access that LAN users have to the Internet.

The Web Site Filter controls and monitors the access users have to web sites. Sites can be blocked on a site-wide or individual basis and by the features a web site uses or content it provides.

This guide is intended for use by the person responsible for installing or managing the network. It assumes knowledge of the following:

- Basic familiarity with Ethernet networks and the Internet Protocol.
- Knowledge of how to install and handle electronically sensitive equipment.



If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

<http://www.3com.com/>

How to Use This Guide

[Table 1](#) shows where to look for specific information in this guide.

Table 1 Where to find specific information

If you are looking for...	Turn to...
A description of the Firewall's features and example applications.	Chapter 1
A description of the Firewall's front and back panel displays and connectors, and installation information.	Chapter 2
A quick setup guide for the Firewall.	Chapter 3
Information on how to configure the Firewall using the Firewall's Web interface.	Chapter 4 - Chapter 10
Information about installing and setting up the Web Site Filter, configuring policy rules and resetting the Firewall.	Chapter 11
Troubleshooting common Firewall problems.	Chapter 12
Information about Denial of Service and other attacks.	Chapter 13
An introduction to TCP/IP, VPNs and Bandwidth Management.	Chapter 14
Important Safety Information.	Appendix A
Technical Specifications of the Firewall.	Appendix B
Cable Specifications.	Appendix C
Information about obtaining Technical Support.	Appendix D

Conventions

[Table 2](#) and [Table 3](#) list conventions that are used throughout this guide.

Table 2 Notice Icons




Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 3 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Commands	<p>The word “command” means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example:</p> <p>To display port information, enter the following command:</p> <p>bridge port detail</p>
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	<p>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:</p> <p>Press Ctrl+Alt+Del</p>
Words in <i>italics</i>	<p>Italics are used to:</p> <ul style="list-style-type: none">■ Emphasize a point.■ Denote a new term at the place where it is defined in the text.■ Identify menu names, menu commands, and software button names. Examples: <p>From the <i>Help</i> menu, select <i>Contents</i>.</p> <p>Click <i>OK</i>.</p>

Terminology

This section lists terminology used in this guide.

DMZ — Demilitarized Zone port. One of the Firewall’s three physical ports. If you connect publicly-accessible servers and workstations to this port, they are accessible from the Internet but still protected from Denial of Service attacks

DoS Attacks — Denial of Service Attacks. An attempt to stop one of your services running, such as a Web or FTP server. There are several kinds of DoS attacks.

High Availability — A feature to provide greater resiliency to device failure, where two Firewalls are deployed in parallel, (active & standby) - should the active Firewall fail, the secondary standby Firewall takes over.

IP address — The Internet Protocol address is the network layer address of a device assigned by the user or network administrator of an IP network. An IP address consists of 32 bits divided into two or three fields: a network number and a host number, or a network number, a subnet number, and a host number.

IP Spoof — A type of DoS attack. An IP spoof uses a fake IP address to bypass security settings which may bar access from the real IP address.

IRC — Internet Relay Chat. Provides a way of communicating in real time with people from all over the world.

ISP — Internet Service Provider. A business that provides Internet access to individuals or organizations.

Firewall — Used in this guide to refer to the SuperStack 3 Firewall.

L2TP — Layer 2 Tunneling Protocol. This protocol is used for native Microsoft VPN clients and is used in conjunction with IPSec (denoted L2TP/IPSec), it can also be used as an authentication method for some broadband Internet Service Providers (ISPs).

Land Attack — A type of DoS attack. In a Land attack, a packet is sent that appears to come from the same address and port that it is sent to. This can hang the machine to which it is sent.

Management Station — This is the workstation from which you run the Web interface for the Firewall.

Web interface — This is the Web-based application which you use to set up the Firewall to protect your network from attack and to control access to the Internet for LAN users.

NAT — Network Address Translation. NAT refers to the process of converting the IP addresses used within a private network to Internet IP addresses.

NTP — Network Time Protocol. This allows the Firewall to automatically set the local time, via an NTP server on the Internet

NNTP — Network News Transfer Protocol. This protocol is used to distribute Usenet news articles over the Internet.

Ping of Death — A type of DoS attack. The Internet Protocol (IP) defines the maximum size for a Ping packet. However, some Ping programs can send packets that are larger than this size which can cause some systems to crash.

PPPoE — PPPoE stands for Point-to-Point Protocol over Ethernet and is based on two widely accepted standards, Point-to-Point Protocol (PPP) and Ethernet. PPPoE is a method for personal computers to connect to a broadband service (typically DSL).

RADIUS — Remote Authentication Dial-in User Service. RADIUS enables network administrators to effectively deploy and manage VPN Client based remote users. The RADIUS server allows multiple users to share a single Group Security Association but require an additional unique password for accounting and access.

SYN Flood — A type of DoS attack. This is where a client opens a connection with a server but does not complete it. If the server queue fills up with partially-open connections, no other clients can make genuine connections to that server.

UTC —stands for Universal Time Co-ordinated, and is the standard time common to all places in the world. It is also commonly referred to as GMT or World Time.

VPN — stands for Virtual Private Network, and is a method of networking that uses data encryption and the public internet to provide secure communications between sites without incurring the expense of leased lines.

Web Site Filter — Used in this guide to refer to the SuperStack 3 Web Site Filter.



See [Chapter 13, "Types of Attack and Firewall Defences"](#) for further information on types of attack and how the Firewall defends against them.

Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- SuperStack 3 Firewall User Guide
- Part Number DUA1611-0AAA0x
- Page 24



Do not use this e-mail address for technical support questions. For information about contacting Technical Support, see [Appendix D](#).

Registration

To register your Firewall point your web browser to

`http://www.3com.com/ssfirewall`

click on *Register Product Now* and follow the instructions.



GETTING STARTED

- [Chapter 1](#) Introduction
- [Chapter 2](#) Installing the Hardware
- [Chapter 3](#) Quick Setup for the Firewall



1

INTRODUCTION

This chapter contains the following:

- [What is the SuperStack 3 Firewall?](#)
- [Firewall and 3Com Network Supervisor](#)
- [Firewall Features](#)
- [Introduction to Virtual Private Networking \(VPN\)](#)

What to Read if You are in a Hurry

If you want to install and get your Firewall running as quickly as possible and then configure the advanced features of your Firewall later, read the following sections in this manual:

- **This chapter** — to get a basic overview of the Firewall's main features.
- [Installing the Hardware](#) — for information about physically installing the Firewall.
- [Quick Setup for the Firewall](#) — For instructions on running the Installation Wizard which configures your Firewall for use on your network.

The information in these three chapters will allow you to complete the installation and basic configuration of your Firewall.

For background information about the Firewall and the networking technologies and concepts used, see the following chapter:

- [Networking Concepts](#) — for information about TCP/IP, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), Port Numbers, Virtual Private Networks (VPNs) and Bandwidth Management.

What is the SuperStack 3 Firewall?

The SuperStack® 3 Firewall is a dedicated firewall appliance which is installed between a Private LAN and a Router. The Firewall is a complete network security system with all hardware and software pre-installed. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The purpose of the Firewall is to allow a private Local Area Network (LAN) to be securely connected to the Internet. You can use the Firewall to:

- Prevent theft, destruction, and modification of data.
- Filter incoming data for unsafe or objectionable content.
- Log events which may be important to the security of your network.

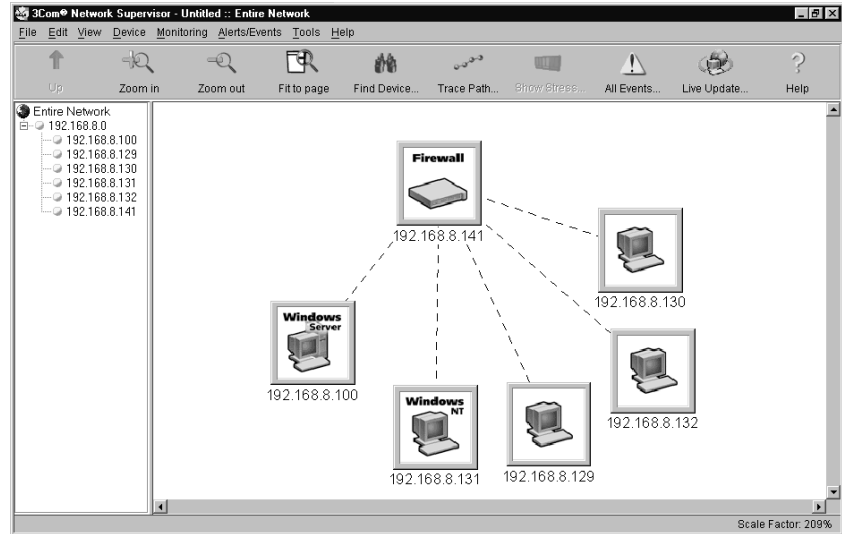
The Firewall has three Ethernet ports which are used to divide the network into separate areas.

- The *Wide Area Network* (WAN) port attaches to the Internet access device, for example, Router or Cable Modem.
- The *Local Area Network* (LAN) port attaches to the local network through hubs and switches. LAN users have access to Internet services such as e-mail, FTP, and the World Wide Web. However, all workstations and data on the LAN are protected from hacker attacks that might come through the WAN port.
- The *Demilitarized Zone* (DMZ) port is used for public servers, such as Web or FTP servers. Machines attached to this port are visible from the WAN port, but are still protected from hacker attacks. Users on the secure LAN port can also access servers on the DMZ port.

Firewall and 3Com Network Supervisor

The Firewall is supplied with a copy of 3Com Network Supervisor. Network Supervisor is a powerful, intuitive network management application for small to medium enterprise networks.

Figure 1 3Com Network Supervisor display



Network Supervisor automatically discovers up to 1500 network devices and shows devices and connections on a graphical display. Network managers can view network activity, monitor stress and set thresholds and alerts. This information helps to provide the most efficient, cost-effective use of network resources.

Version 3.0 and later releases add significant extra functionality designed to detect network inefficiency and optimize network performance. Features include support for related and recurring events, user definable reports, auto-alerting using pager or SMS messages and simple updates from the 3Com web site.

3Com Network Supervisor offers the following support to Firewall users:

- If your 3Com Network Supervisor management station is located on the LAN, it discovers the Firewall automatically and displays it on the topology map.
- The topology map indicates that the Firewall is a 3Com Firewall and uses an appropriate icon to represent it.

- Double-clicking on the Firewall icon launches the Web interface of the Firewall.

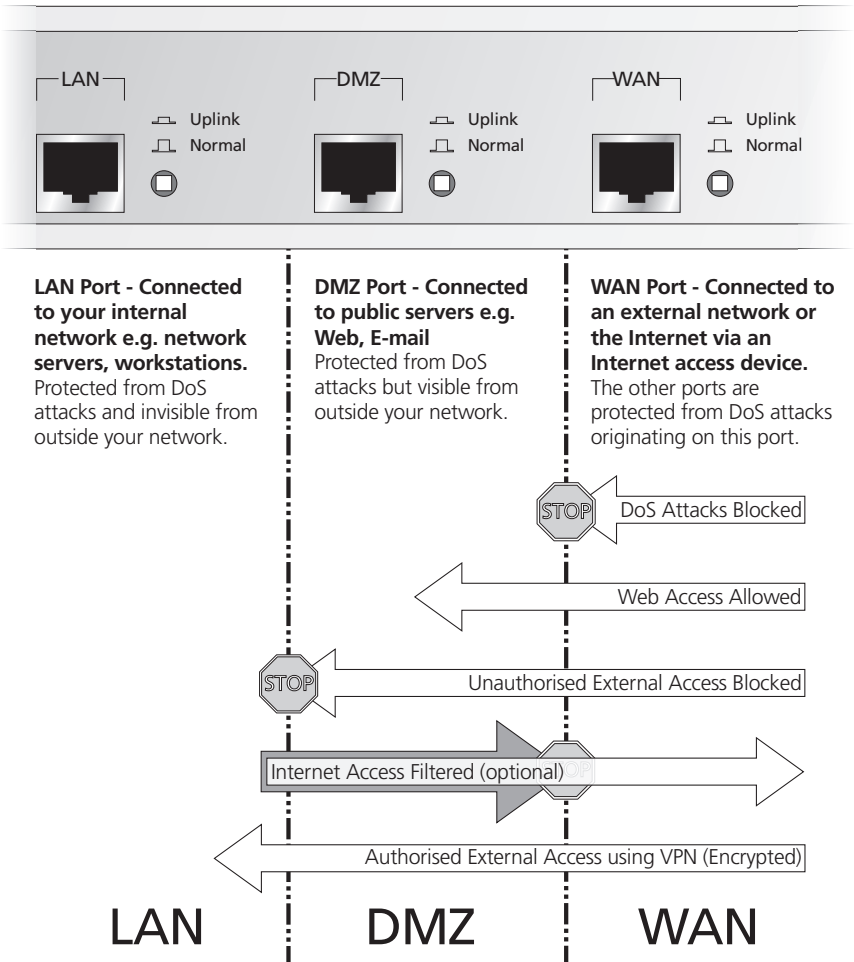
If your 3Com Network Supervisor management station is located on the WAN side of the Firewall you must follow the steps below before Network Supervisor can detect your Firewall:

- 1 Access the Web interface from a Web browser connected to the LAN port of the Firewall.
- 2 Click *Policy*, after the Management screen appears.
- 3 Click on the *User Privileges* tab.
- 4 Add a user to the *Current Privileges* list. Enter the user name in the *User* field.
- 5 Click on *Remote Access* and click *Update Privileges*.

Firewall Features This section lists the features of the Firewall.

Firewall Security The Firewall is preconfigured to monitor Internet traffic, and detect and block *Denial of Service (DoS)* hacker attacks automatically. Refer to [Figure 2](#).

Figure 2 Firewall Security Functions - Default Firewall Policy



The Firewall examines every packet that comes from outside the LAN and discards any packet that has not been authorized from inside the LAN. This is known as stateful packet inspection.

Users on the LAN have access to all resources on the Internet that are not blocked by any of the filters.

Users on the Internet can access hosts on the DMZ, such as a Web server, but cannot access any resources on the LAN unless they are authorized remote users.

The Firewall protects your network against the following Denial of Service attacks:

- Ping of Death
- Smurf Attack
- SYN Flood
- LAND Attack
- IP Spoofing
- Teardrop

To find more information on DoS and other attacks refer to [Chapter 13, “Types of Attack and Firewall Defences”](#)

Advanced users can extend the security functions of the Firewall by adding network access rules and user privileges. See [“Adding and Editing Policy Rules”](#) on [page 119](#) and [“Configuring Users”](#) on [page 123](#) for more information.

Web URL Filtering

You can use the Firewall to monitor and control user access to public web sites, through blocking and logging inappropriate content. See [“Configuring the Filtering Options”](#) on [page 79](#) for more information.

The Firewall supports a range of filtering options, designed to offer choice in which customers choose to police Internet web usage.

Manual Filtering — The Firewall supports manual web filtering, where an administrator explicitly defines what websites are permitted, or alternatively which websites are defined *not acceptable for business usage*. These can be defined in various ways, for example specifying web URL's in a denied (black list) or listing permitted URL's in permitted (white list).

In addition to specifying specific URL's, administrators can define URL keywords which should be blocked, which can further fine-tune black or

white URL lists, for example blocking keywords such as *job* will prevent most websites employment pages, or XXX will capture a large number of websites containing pornographic material.

Embedded Filtering Service — The optional 3Com Web Site Filter service, extends the capabilities of manual filtering, where an administrator defines what content categories are deemed unacceptable to company policy. This is an annual service which works by downloading a database of URLs on a regular (weekly) basis, this database is broken into 12 different content categories, which is maintained on behalf of 3Com by a company called SurfControl, who use a team of editors to continually seek and categorize new websites.

The key advantage of this filtering service is that it is extremely simple to enable and configure, it is performed on the Firewall itself, eliminating the need for any additional software or hardware.

3rd Party Content Filtering — The Firewall also supports 3rd party filtering services. Currently two 3rd party vendors products are supported, N2H2 and Websense Enterprise. To deploy this type of content filtering, a separate server is required running the 3rd party filtering software, the Firewall then communicates with this 3rd party application to determine whether a web page should be served or blocked.

High Availability Given the mission critical nature of many Internet connections each component involved in your connection must be highly reliable. The *High Availability* function of your Firewall adds to the already reliable platform eliminating downtime due to hardware failure.

To use the *High Availability* function, connect another SuperStack 3 Firewall to the first as a high availability pair and configure the backup Firewall to monitor the primary Firewall. In the event of failure of the primary Firewall, the backup Firewall takes over its functions. See [“Configuring High Availability”](#) on [page 179](#) for details.

Logs and Alerts The Firewall maintains a log of all events that could be seen as security concerns. It can also track key events such as the top 25 most accessed Web sites, or the top 25 users of Internet bandwidth. You can also set up the Firewall to send an alert message through e-mail when a high-priority concern, such as a hacker attack, is detected. See [“Logs and Alerts”](#) on [page 95](#) for more information.

For detailed logging 3Com recommends that you use a syslog server or a syslog reporting tool. A free syslog server is available from 3Com. To download it point your web browser to:

`http://www.3com.com/ssfirewall`

and follow the *Downloads, Utility Software* link to the *Syslog Server*.

User Remote Access (from the Internet)

Users can access intranet resources on the private LAN by successfully logging into the Firewall from the Internet. Logging in requires a valid user name and password, which are transmitted to the Firewall by the remote user, using a Web browser, through an MD5-based encrypted authentication mechanism. Once logged in, remote users are able to access all IP resources on the LAN

Automatic IP Address Sharing and Configuration

The Firewall provides sharing of a single public IP address through *Network Address Translation (NAT)*. It also provides simplified IP address administration using the *Dynamic Host Configuration Protocol (DHCP)*.

NAT automatically translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. It enables the Firewall to be used with broadband modems and with low cost Internet accounts where only one IP address is provided by the ISP. See [“Network Address Translation \(NAT\)”](#) on [page 218](#) and [“Dynamic Host Configuration Protocol \(DHCP\)”](#) on [page 219](#) for more information.

The DHCP server automatically assigns all PCs on the LAN with the correct IP information. The DHCP client allows the Firewall to acquire the correct IP settings from the ISP. See [“Specifying DMZ Addresses”](#) on [page 67](#) for more information.

Introduction to Virtual Private Networking (VPN)

The Firewall includes support for IPSec Virtual Private Networking. This section provides an introduction to Virtual Private Networking (VPN).

Virtual Private Networking

Today's business environment requires close, real-time collaboration with trading partners, legal, and financial advisors, as well as remote workers and branch offices. This “real-time” requirement often leads to the creation of an “extranet” where branch offices and partners are connected to a primary network in one of two ways:

- Leasing dedicated data lines to connect all sites.
- Using the public Internet to connect all sites and remote users together.

Each of these methods has its benefits and drawbacks. Establishing a leased line connection between the sites offers a dedicated, secure access but at a very high cost.

The other option is to use an existing Internet connection to transmit data unencrypted over the public Internet network. While this option is less expensive and can provide higher performance, it is much less secure than dedicated site-leased lines.

VPN uses data encryption and the public Internet to provide secure communications between sites without incurring the huge expense of site to site leased lines.

The Firewall embodies different levels of encryption that can be used to create a VPN tunnel. For the tunnel to work correctly, the terminating device at the other end of the tunnel must be using the same level and type of encryption. See [“Configuring Virtual Private Network Services”](#) on [page 151](#) for more details.

2

INSTALLING THE HARDWARE

This chapter contains the following:

- [Before You Start](#)
- [Positioning the Firewall](#)
- [Firewall Front Panel](#)
- [Firewall Rear Panel](#)
- [Redundant Power System \(RPS\)](#)
- [Attaching the Firewall to the Network](#)



WARNING: Before installing the Firewall, you must read the safety information provided in [Appendix A](#) of this User Guide.



AVERTISSEMENT: Avant d'installer le Firewall, lisez les informations relatives à la sécurité qui se trouvent dans [l'Appendice A](#) de ce guide.



VORSICHT: Bevor Sie den Firewall hinzufügen, lesen Sie die Sicherheitsanweisungen, die in [Anhang A](#) in diesem Handbuch aufgeführt sind.

Before You Start

Your SuperStack® 3 Firewall (3CR-15110-95) comes with the following:

- A power cord for use with the Firewall.
- Four rubber feet.
- Mounting Kit for a 19 in. rack mount cabinet comprising:
 - two mounting brackets.
 - four screws.
- A SuperStack 3 Firewall User Guide (this guide).
- A SuperStack 3 Firewall CD.

- Warranty Information.
- Software License Agreement.

Positioning the Firewall

When installing the Firewall, make sure that:

- Cabling is located away from:
 - sources of electrical noise such as radios, transmitters and broadband amplifiers.
 - power lines and fluorescent lighting fixtures.
- The Firewall is accessible and cables can be connected easily.
- Water or moisture cannot enter the case of the Firewall.
- Air flow is not restricted around the Firewall or through the vents in the side of the Firewall. 3Com recommends that you provide a minimum of 25 mm (1 in.) clearance.
- Air temperature around the Firewall does not exceed 40 °C (104 °F).

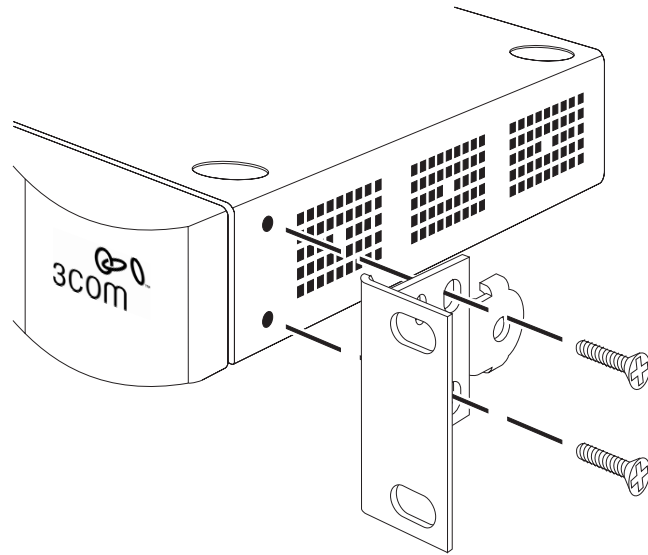


If the Firewall is installed in a 19-inch rack or closed assembly its local air temperature may be greater than room ambient temperature.

- The air is as free from dust as possible.
- The unit is installed in a clean, air conditioned environment.
- No more than four SuperStack 3 units are placed on top of one another, if the units are free-standing.
- The Firewall is situated away from sources of conductive (electrical) dust, for example laser printers.
- The AC supply used by the Firewall is separate to that used by units that generate high levels of AC noise, for example air conditioning units and laser printers.

Rack Mounting the Units

The Firewall is 1U high and will fit a standard 19-inch rack.

Figure 3 Fitting the Rack Mounting Bracket

CAUTION: *Disconnect all cables from the unit before continuing. Remove the self-adhesive pads from the underside of unit, if already fitted.*

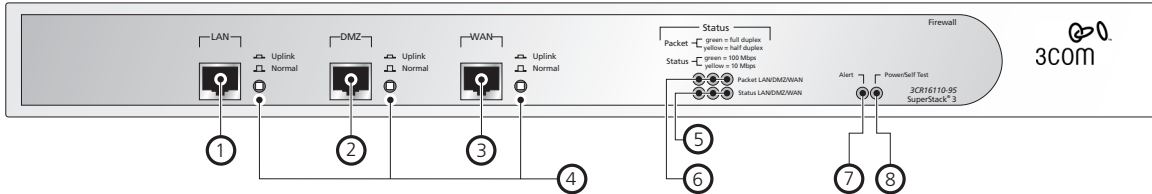
- 1 Place the unit the right way up on a hard, flat surface with the front facing towards you.
- 2 Locate a mounting bracket over the mounting holes on one side of the unit (refer to [Figure 3](#)).
- 3 Insert the two screws supplied in the mounting kit and fully tighten with a suitable screwdriver.
- 4 Repeat the steps 2 and 3 for the other side of the unit.
- 5 Insert the unit into the 19-inch rack and secure with suitable screws (not provided).
- 6 Reconnect all cables.

Securing the Firewall with the Rubber Feet

The four self-adhesive rubber feet prevent the Firewall from moving around on the desk. Only stick the feet to the marked areas at each corner of the underside of the unit if you intend to place the unit directly on top of the desk.

Firewall Front Panel [Figure 4](#) shows the front panel of the Firewall.

Figure 4 Firewall Front Panel



WARNING: *RJ-45 Ports. These are shielded RJ-45 data sockets. They cannot be used as standard traditional telephone sockets, or to connect the unit to a traditional PBX or public telephone network. Only connect RJ-45 data connectors, network telephony systems, or network telephones to these sockets.*

Either shielded or unshielded data cables with shielded or unshielded jacks can be connected to these data sockets.

The Firewall front panel contains the following components:

- 1 LAN Port** - Use a Category 5 cable with RJ-45 connectors. Connect this port to any workstation or network device that has a 10BASE-T or 100BASE-TX port.
- 2 DMZ Port** - Use a Category 5 cable with RJ-45 connectors. Use this port to connect the Firewall to any workstation, server, or network device that has a 10BASE-T or 100BASE-TX port.
- 3 WAN Port** - Use a Category 5 cable with RJ-45 connectors. Connect this port to any Internet access device that has a 10BASE-T or 100BASE-TX port.
- 4 Normal/Uplink Switches** - The setting of these switches determines the operation of each port. See [“Attaching the Firewall to the Network”](#) on [page 37](#) for more information about setting these switches.
- 5 Status LEDs** - The WAN, LAN, and DMZ ports each have a Status LED that indicates the following:
 - *Green* indicates that the link between port and the next network device is operational at 100 Mbps.
 - *Yellow* indicates that the link between the port and the next network device is operational at 10 Mbps.

- *Off* indicates that nothing is operational or that the link to the port has failed.
- 6 Packet LEDs** - The WAN, LAN, and DMZ ports each have a Packet LED that indicates the following:
- *Green* indicates that data is being transmitted/received on this port in full-duplex mode.
 - *Yellow* indicates that data is being transmitted/received on this port in half-duplex mode.
 - *Off* indicates that no traffic is being passed.
- 7 Alert LED** - This LED shows orange to alert you of the following:
- A failure in the self-test the Firewall runs when switched on.
 - No operational firmware is currently loaded.
 - Potential attacks on your network.
 - An attempt to access a restricted site.
 - A hacker attack or access to a restricted service.
- 8 Power/Self Test LED** - This LED shows green to indicate that the unit is switched on. This LED flashes for about 90 seconds while self-test is running, and also when restarting.

If you have installed a 3Com RPS unit with the Firewall and the RPS has a fault, the Power LED flashes to warn you. Once the fault on the RPS has been rectified, the Power LED stops flashing.

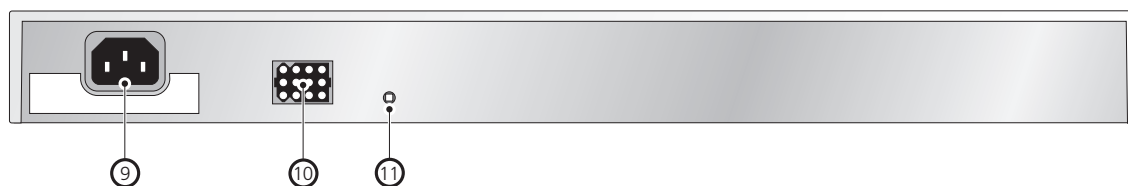


To diagnose faults see [“Troubleshooting”](#) on [page 203](#).

Firewall Rear Panel

[Figure 5](#) shows the rear panel of the Firewall.

Figure 5 Firewall Rear Panel



The Firewall rear panel contains the following components:

- 9 Power socket** - Only use the power cord supplied with the Firewall.
- 10 Redundant Power System socket** - Use this connector to attach a Redundant Power System to the Firewall.
- 11 Reset Switch** (recessed) - Use to reset the Firewall.



CAUTION: Holding the Reset Switch when you power on the Firewall erases the operational firmware and return the device to factory default settings. To reset the Firewall see [“Restarting the Firewall”](#) on [page 105](#).

Redundant Power System (RPS)

The SuperStack 3 Advanced Redundant Power System (RPS) offers you the flexibility to supply power to your SuperStack devices in the event of a failure of an internal power supply. The System is a group of products from which you choose the most suitable for your equipment and its configuration. One RPS unit can supply up to eight SuperStack 3 units.

The RPS status is displayed in the *Unit Status* screen on the Web interface.

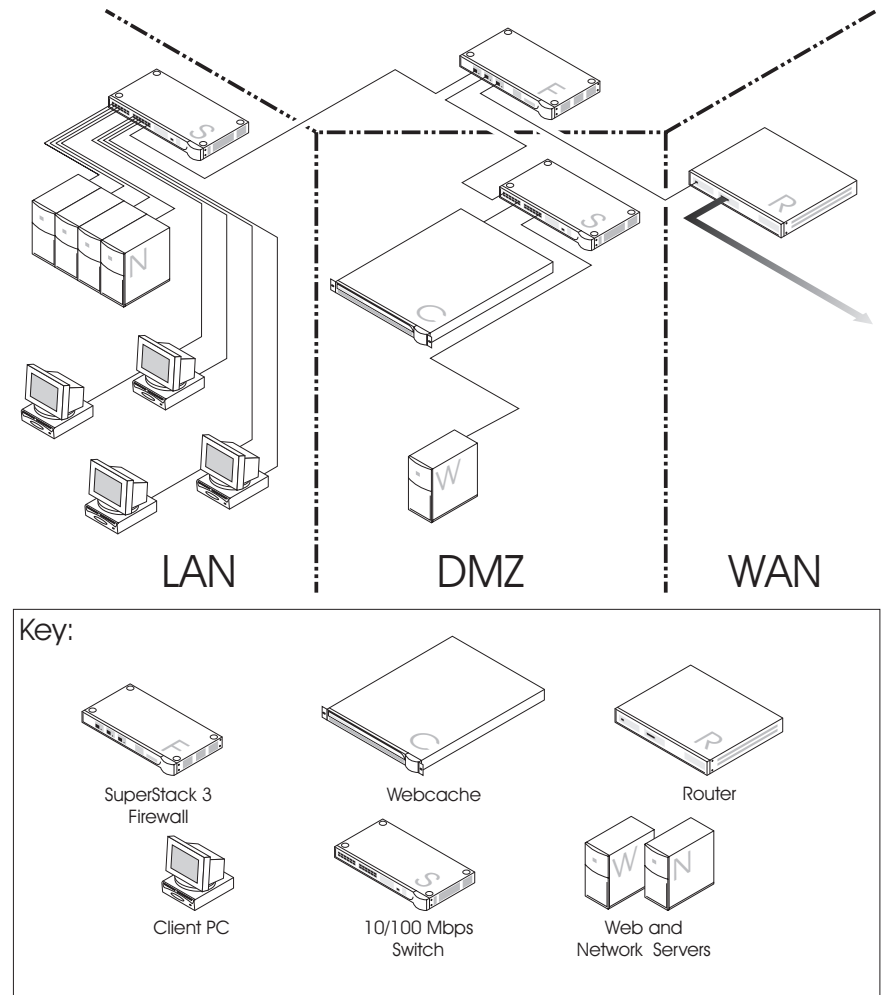
Use the following SuperStack 3 RPS with the Firewall:

- SuperStack 3 - Advanced RPS (3C16071)
- and 60W RPS Power Module - (3C16072)

Attaching the Firewall to the Network

[Figure 6](#) illustrates one possible network configuration.

Figure 6 Network Connection Diagram Showing Sample Network



Never connect two ports on the Firewall to the same physical network. For example, never connect the LAN and DMZ ports into the same device as this bypasses all firewall functions.

To attach the Firewall to your network:

- 1 Connect the Ethernet port labeled WAN on the front of the Firewall to the Ethernet port on the Internet access device.

Refer to the documentation for the Internet access device to find out the configuration of its Ethernet port. If it has an MDIX (normal) configuration, then you can use a standard Category 5 cable.

Make sure that the Uplink/Normal switch is in the **Uplink** position for a standard CAT-5 cable. If you are connecting the WAN port to a hub or switch with a crossover cable, or directly to a workstation with standard cable, make sure the Uplink/Normal switch is in the **Normal** position.

- 2 Connect the Ethernet port labeled LAN to your LAN.

If you are connecting the LAN port to a hub or switch using a standard Category 5 UTP cable, make sure that the Uplink/Normal switch for the LAN port is in the **Uplink** position. If you are connecting the LAN port to a hub or switch with a crossover cable, or directly to a workstation with standard cable, make sure the Uplink/Normal switch is in the **Normal** position.

- 3 Connect the Ethernet port labeled DMZ to the public servers.

If you are installing the Firewall DMZ and want to protect the public servers, such as Web and FTP servers, use the DMZ port. If you are connecting the DMZ port directly to a server using standard Category 5 cable, make sure that the Uplink/Normal switch is in the **Normal** position. If you are connecting the DMZ port to a switch using standard Category 5 cable, make sure that the Uplink/Normal switch is in the **Uplink** position.

- 4 Turn on or restart the Internet access device.
- 5 Plug the Firewall into an AC power outlet, and then plug the power supply output cable into the power adapter socket.
- 6 Wait for the Power LED to stop flashing.

The Firewall is designed to start up as soon as power is supplied to it. Then it runs a series of self-diagnostics to check for proper operation. During these diagnostics, which take about 90 seconds, the Power LED flashes.



CAUTION: Do not switch the Firewall off and on quickly. After switching it off, wait approximately five seconds before switching it on again.

- 7 Make sure that the Status LEDs are on for all ports that are connected. If not, see [Chapter 12](#) for troubleshooting information.

The Firewall is now attached to the network.



By default, no traffic that originates from the Internet is allowed onto the LAN, and all communications from the LAN to the Internet are allowed. That is, all inbound connections are blocked and all outbound connections are allowed.

You can now configure the Firewall. See the following chapters for more information:

- [Chapter 3](#) for a quick setup guide for the Firewall.
- Chapters 4 to 10 for full information about all the configuration options.
- [Chapter 11](#) for information about the Web Site Filter and Network Access Policy Rules.

At frequent intervals, check the Firewall for the following:

- The Alert LED is not continuously lit — if it is, there are problems on your network.
- The case vents are not obstructed.
- The cabling is secure and is not pulled taut.

3

QUICK SETUP FOR THE FIREWALL

This chapter contains the following:

- [Introduction](#)
- [Setting up a Management Station](#)
- [Configuring Basic Settings](#)
- [Configuring WAN Settings](#)
- [Configuring LAN Settings](#)
- [Confirming Firewall Settings](#)

Introduction

The first time the Firewall is started it runs an *Installation Wizard*. The Installation Wizard asks you questions about your network and configures the Firewall so that it works in your network.



If you later move your Firewall to another network and want to use the Installation Wizard to configure the Firewall you can activate the Installation Wizard manually. To start the Installation Wizard manually, click Tools, then the Configuration tab, then select Wizard.

The configuration process can be split into three steps

- 1 To access the Installation Wizard you must first configure a computer as a *Management Station*. See [“Setting up a Management Station”](#) on [page 42](#) for details.
- 2 Launch a web browser on the Management Station and enter `http://192.168.1.254` to browse the Firewall.
- 3 Follow the instructions supplied by the Installation Wizard and answer the questions it asks.

The process followed by the Installation Wizard is described in the following sections:

- [Configuring Basic Settings](#)
- [Configuring WAN Settings](#)
- [Configuring LAN Settings](#)
- [Confirming Firewall Settings](#)

Setting up a Management Station

The Firewall has the following default settings:

- IP address — 192.168.1.254
- Subnet mask — 255.255.255.0

To access the Installation Wizard you must configure a computer to be in the same subnet. This computer will be referred to as a Management Station.

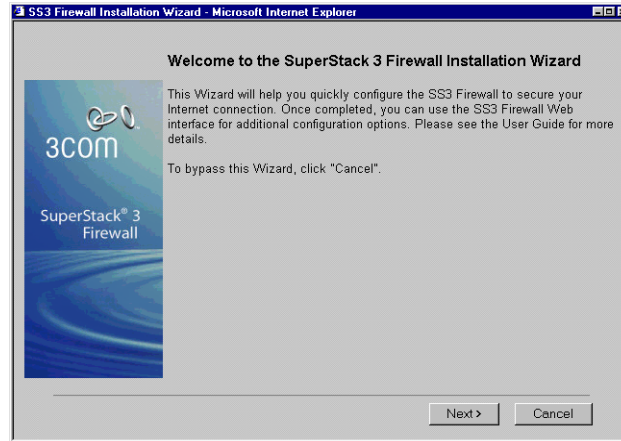
Follow the steps below to configure a computer as a Management Station:

- 1** Note the IP address and subnet mask of the Management Station. You will need to return your Management Station to these settings when you have finished using the Installation Wizard.
- 2** Change the IP address to a value within the Firewall's default subnet. This will be a value between **192.168.1.1** and **192.168.1.254** but not **192.168.1.254** as this is already taken by the Firewall. A suitable address would be **192.168.1.20** if this is not already taken by another device.
- 3** Enter **http://192.168.1.254/** (the Firewall's default IP address) into the box at the top of the browser window. The Installation Wizard is displayed on screen and guides you through the configuration described in the sections below.
- 4** Remember to change the IP address and subnet mask of your Management Station back to their original values when you have finished configuring the Firewall using the Installation Wizard.

Configuring Basic Settings

When the Installation Wizard first starts it displays a welcome screen shown in [Figure 7](#).

Figure 7 Installation Wizard Startup Screen



Click *Next* to start configuring your Firewall using the Installation Wizard.



If you want to configure your Firewall manually, click Cancel. You are then returned to the Web interface. See ["Configuring the Firewall"](#) starting on [page 55](#) to configure the Firewall using the Web interface.

Setting the Password

The *Set Your Password* screen is displayed as shown in [Figure 8](#). Choose an administration password and enter it in the *New Password* and *Confirm New Password* fields. This is used in conjunction with the **admin** User Name when logging on to the Firewall in the future.

Figure 8 Set Password Screen

Click *Next* to continue.

Setting the Time Zone

Select the *Time Zone* appropriate to your location and click *Next* to continue. The *Time Zone* you choose affects the time recorded in the logs.

Figure 9 Set Time Zone screen

This completes the Basic setup of the Firewall.

The Firewall now attempts to configure some of its network settings automatically. If it is unable to detect the settings automatically, the *Installation Wizard* prompts you for the required settings.

Configuring WAN Settings

The Installation Wizard detects if the Firewall has been automatically allocated an address for its WAN port.

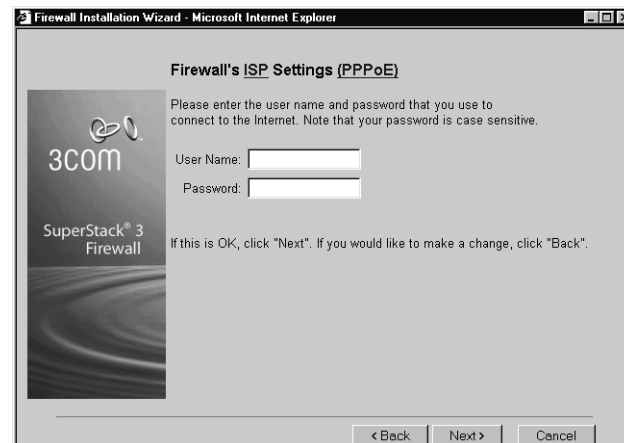
- If the Firewall has been allocated an IP address then it attempts to configure itself automatically. See [“Automatic WAN Settings”](#) below.
- If the Firewall has not been allocated an IP address then it prompts you for the settings it requires. See [“Manual WAN Settings”](#) on [page 45](#).

Automatic WAN Settings

The Installation Wizard checks for the presence of a DHCP Server or a PPPoE server on the WAN port. Depending on the server found the Firewall configures itself appropriately as described below:

- *DHCP Server* — The Firewall requests an IP address from the DHCP server on the WAN Port and uses the IP address, subnet mask and any DNS information supplied
- *PPPoE Server* — The Installation Wizard prompts you to enter the User Name and Password supplied by your ISP. See [Figure 10](#).

Figure 10 Configuring the Firewall's PPPoE settings



If the WAN Setup has completed successfully, go to [“Configuring LAN Settings”](#) on [page 51](#).

Manual WAN Settings

If the Installation Wizard is unable to detect an automatic address server on the WAN Port or if the WAN port is not connected it displays a dialog box informing you of this and offers the choice of:

- Connecting your Firewall (if not already connected) and restarting the Installation Wizard.
- Configuring your Firewall manually.

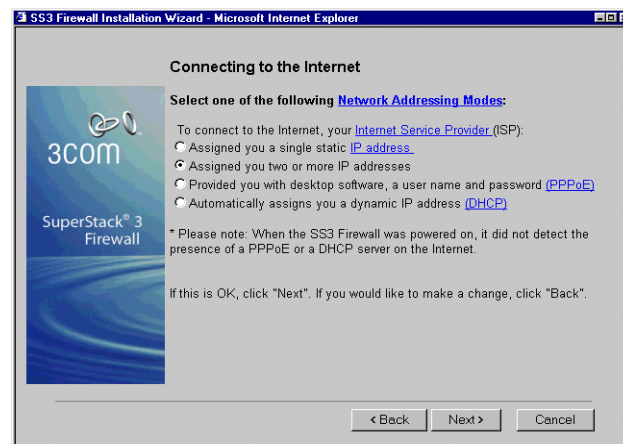
If you want to try to configure your Firewall again using the Installation Wizard's automatic detection then:

- 1 Disconnect the power cord from the Firewall.
- 2 Wait at least 5 seconds.
- 3 Reconnect the power cord.
- 4 Enter the Firewall's IP address in your browser.

If you want to configure the WAN settings of the Firewall manually then click *Next* to continue.

The Installation Wizard displays its *Connecting to the Internet* screen, shown in [Figure 11](#). This allows you to specify the addressing mode you are using on your WAN port.

Figure 11 Specifying the connection on the WAN port



The options are as follows:

- [Using a Single Static IP Address](#) — This address must be taken by the Firewall's WAN port to allow devices connected to the LAN port to communicate with devices connected to the WAN port. Network Address Translation (NAT) is enabled.

- [Using Multiple Static IP Addresses](#) — One address is taken by Firewall's WAN port. NAT can be disabled sharing the addresses between the DMZ port and the LAN port or enabled leaving all the public addresses for the DMZ port. This option is offered later in the *Installation Wizard*.
- [Using an IP Address provided by a PPPoE Server](#) — One IP address is provided by the PPPoE server. This is taken by the WAN port. Network Address Translation (NAT) is enabled.
- [Using a Static IP address provided by a DHCP Server](#) — One IP address is provided by the DHCP server. This is taken by the WAN port. Network Address Translation (NAT) is enabled.

The settings for each of these options are detailed in the following sections.

Using a Single Static IP Address

Select *Assigned you a single static IP address* and click *Next*. You are reminded that NAT will be enabled. Click *Next* to display the *Getting to the Internet* screen shown in [Figure 12](#).

Figure 12 Configuring the Firewall

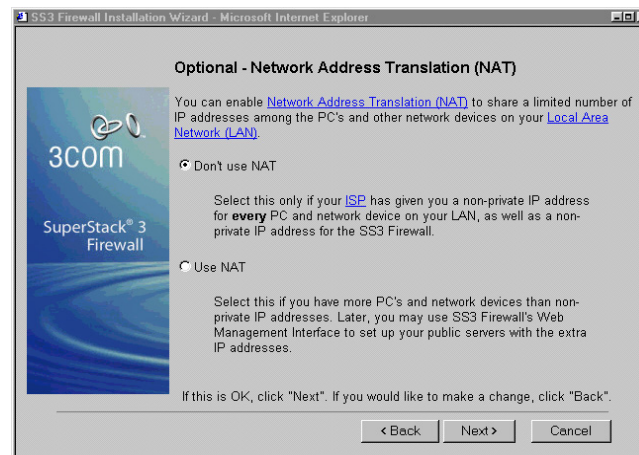
To configure the WAN networking of your Firewall enter the following

- 1 In the *Firewall WAN IP Address* field enter the single address which has been allocated to your Firewall. Enter the subnet mask for the above IP address in the *WAN/DMZ Subnet Mask* field.
- 2 In the *WAN Gateway (Router) Address* field enter the address of your internet access device. This may be a router, LAN modem or other device and must be in the same subnet as the WAN IP address of the Firewall.
- 3 Enter any DNS servers external to your network in the order that you want them to be accessed. The second server is only accessed if the first is unavailable or is unable to answer your query.
- 4 Click *Next* to proceed to the final part of the configuration. See [“Configuring LAN Settings”](#) on [page 51](#).

Using Multiple Static IP Addresses

Select *Assigned you two or more IP addresses* and click *Next*. The *Network Address Translation* screen is displayed as shown in [Figure 13](#).

Figure 13 Choosing whether to activate NAT for multiple addresses



You are given a choice of:

- Don't use NAT — This disables Network Address Translation, limiting you to the same number of IP devices as you have addresses.
- Use NAT — This enables Network Address Translation allowing you to use as many IP devices as you wish on the LAN port. The Firewall uses one public IP address and the remaining public IP addresses can be allocated to devices on the DMZ port.

Click *Next* to proceed to the *Getting to the Internet* screen shown in [Figure 14](#).

Figure 14 Setting the Firewall WAN configuration

The *Getting to the Internet* screen contains the following fields:

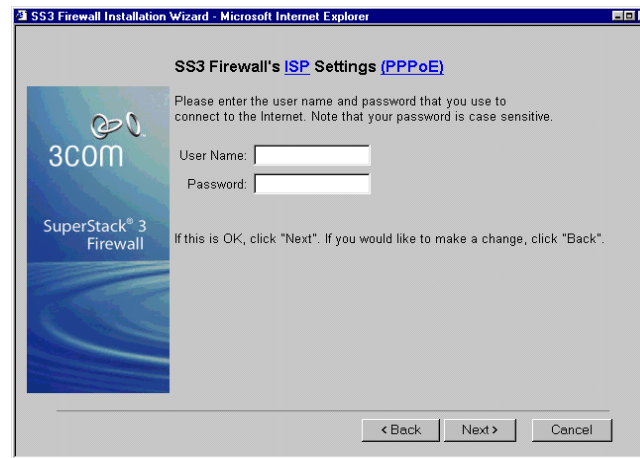
- 1 *Firewall WAN IP Address* — Choose one of the addresses allocated by your ISP as the address of the Firewall's WAN port. This is used for communication across the Firewall and to manage the Firewall remotely.
- 2 *WAN/DMZ Subnet Mask* — Enter the subnet mask that defines the IP address range supplied by your ISP.
- 3 *WAN Gateway (Router) Address* — Enter the IP address of your route or internet access device. This must be in the same address range as the *WAN IP Address*.
- 4 *DNS Server Address* — Enter the IP address of your ISP's DNS server in this field. This is used to resolve machine names to IP addresses. If you have access to additional DNS Servers, enter them in the *Optional Second DNS Server Address* and *Optional Third DNS Server Address* fields. These are accessed if the first stated DNS server does not respond or if it has no record of a device name.

Click *Next* to proceed to the final part of the configuration. See ["Configuring LAN Settings"](#) on [page 51](#).

Using an IP Address provided by a PPPoE Server

Select the *Provided you with desktop software, a user name and password* option and click *Next*. The *Firewall's ISP Settings (PPPoE)* screen is displayed as shown in [Figure 15](#).

Figure 15 Configuring the Firewall's PPPoE settings



Enter the *User Name* and *Password* as supplied by your ISP and click *Next* to proceed to the final part of the configuration. See ["Configuring LAN Settings"](#) on [page 51](#).

Using a Static IP address provided by a DHCP Server

Select the *Automatically assigns you a dynamic IP address (DHCP)* option and click *Next*. If a DHCP server is detected the Firewall obtains its IP address automatically and enables NAT for all devices connected to the LAN port. Click *Next* again to confirm your choice and proceed to the final part of the configuration. See ["Configuring LAN Settings"](#) below.

Configuring LAN Settings

Once the WAN setting of the Firewall have been configured, the *Installation Wizard* configures the Firewall's LAN settings. Some of the following processes are optional and screens only appear if they are relevant to the configuration of your Firewall.

Automatic LAN Settings

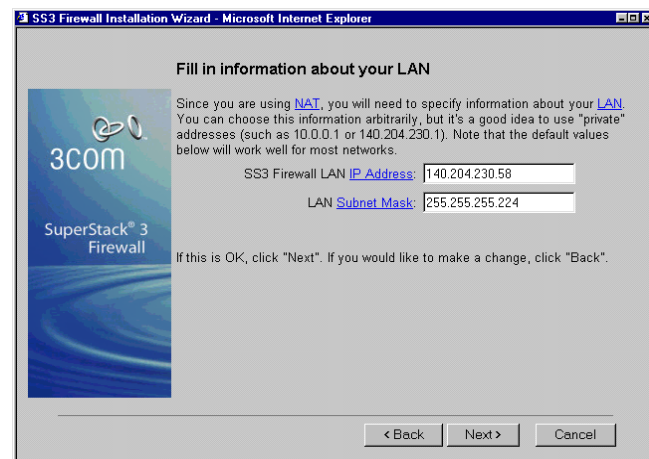
The *Installation Wizard* checks for the presence of a DHCP server on the LAN port.

- If there is no DHCP server found on the network connected to the LAN port then the Firewall's DHCP server is activated allowing automatic address configuration on your LAN.
- If there is a DHCP server found on the network connected to the LAN port then the Firewall deactivates its DHCP server. This prevents the Firewall giving out addresses that will conflict with those allocated by another server.

Entering information about your LAN

If you are using NAT the *Fill in information about your LAN* screen is displayed as shown in [Figure 16](#). If you are not using NAT this screen is not displayed as these settings are the same as the WAN settings.

Figure 16 Configuring LAN Settings



- Choose an IP address for the LAN port of your Firewall and enter it in the *Firewall LAN IP Address* field.
- Enter the Subnet mask for your LAN network in the *LAN Subnet Mask* field.



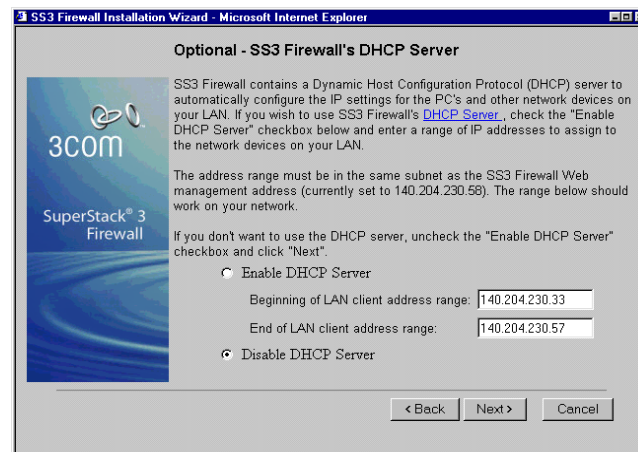
The default IP address of the Firewall is 192.168.1.254 with a subnet mask of 255.255.255.0. You may want to keep this setting as other 3Com products also have their default addresses in this range.

Click *Next* to continue.

Configuring the DHCP Server

If a DHCP server has been detected on your LAN network then the Firewall disables its own DHCP server and this screen is not displayed. Otherwise the Firewall's DHCP Server screen is displayed as shown in [Figure 17](#).

Figure 17 Configuring the Firewall's DHCP Server



If you want to use the Firewall as a DHCP server to automatically provide IP addresses for the computers on your LAN click the *Enable DHCP Server* box and set the range of addresses you want it to allocate.



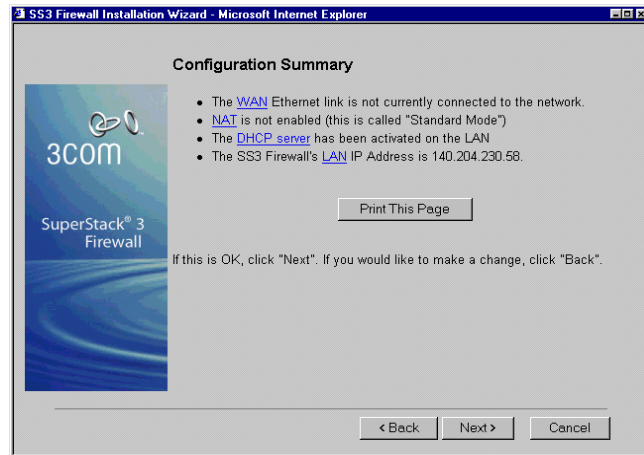
The addresses you set must be contained entirely within your LAN subnet and must be currently unused.

Click *Next* to continue. The Firewall now reviews its settings. See [“Confirming Firewall Settings”](#) below for details.

Confirming Firewall Settings

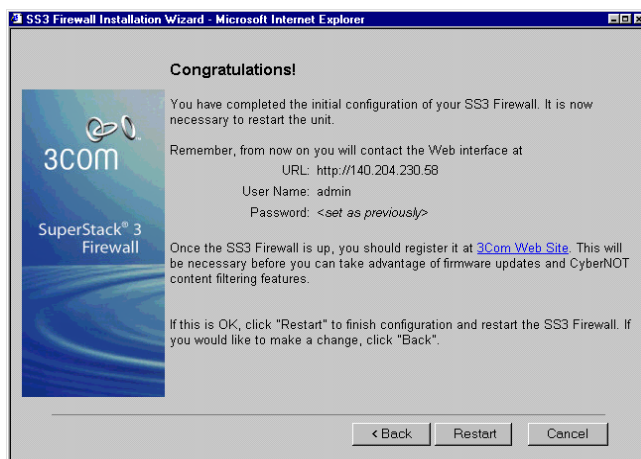
The Firewall prompts you to confirm the settings it has established through automatic configuration as well as those entered manually. You are presented with a screen similar to [Figure 18](#) showing you settings with which the Firewall has been configured.

Figure 18 Firewall Configuration Summary



- If you want to keep a hard copy of this page click *Print This Page*.
- To accept the settings click *Next*.
- To change the configuration of the Firewall click *Back*.
- If you want to configure the Firewall manually:
 - Click *Cancel* to lose the changes made by the Installation Wizard or
 - Click *Next*, continue to the end of the Installation Wizard and make the changes once the Firewall has reset

If you click *Next* the screen shown in [Figure 19](#) opens.

Figure 19 Congratulations Page

Click *Restart* to complete the configuration of the Firewall using the *Installation Wizard*.

The Firewall takes under a minute to restart during which time the Power/Self test LED flashes. When the Power/Self test LED stops flashing the Firewall is ready for use.



CONFIGURING THE FIREWALL

- [Chapter 4](#) Basic Settings of the Firewall
- [Chapter 5](#) Setting up Web Filtering
- [Chapter 6](#) Using the Firewall Log And Tools Options
- [Chapter 7](#) Setting a Policy
- [Chapter 8](#) Advanced Settings
- [Chapter 9](#) Configuring Virtual Private Network Services
- [Chapter 10](#) Configuring High Availability



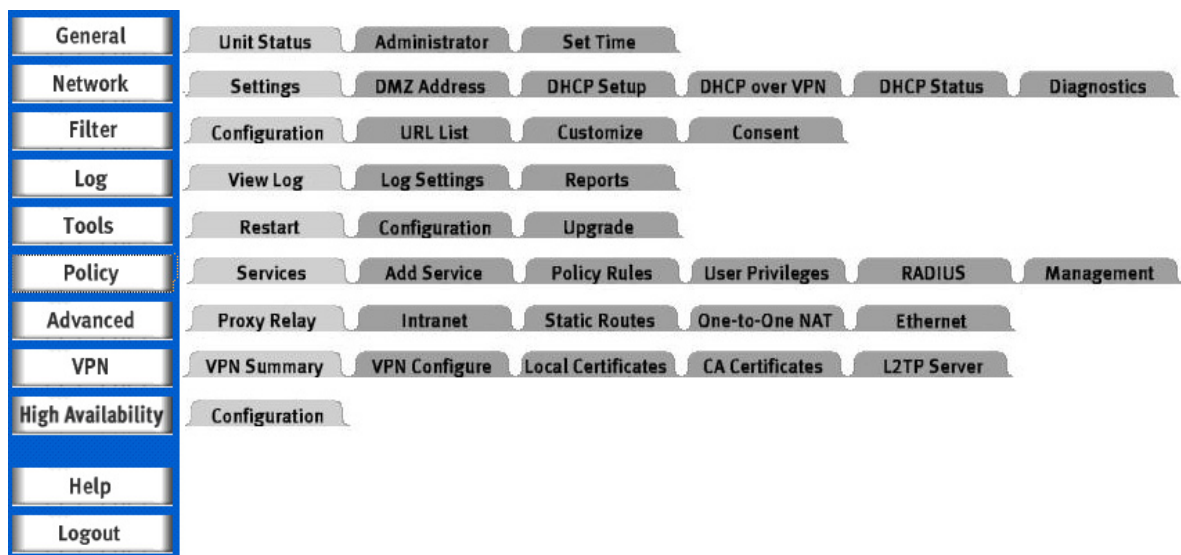
4

BASIC SETTINGS OF THE FIREWALL

Chapters 4 to 10 describe in detail, each of the management operations available from the Firewall's web interface. You can access these operations using a Web browser.

Refer to [Figure 20](#) for menu structure details of the Web interface of the Firewall.

Figure 20 Tree Diagram of the menu structure



The descriptions of these menu options are split into chapters as follows:

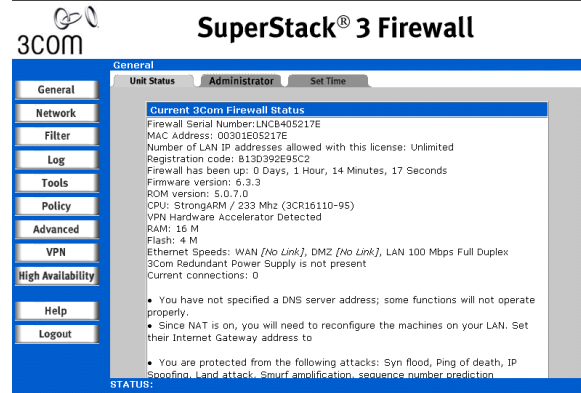
- [Chapter 4](#) — This chapter describes the functions available in the *General* and *Network* menus of the Web interface. These functions are used to configure the Firewall for your network and location and are most frequently accessed when setting up or moving the Firewall or reconfiguring it for another role.

- [Chapter 5](#) — [“Setting up Web Filtering”](#) on [page 79](#) describes the functions available in the *Filter* menu of the Web interface. These functions allow you to control the access your users have to information on the Web.
- [Chapter 6](#) — [“Using the Firewall Log And Tools Options”](#) on [page 95](#) describes the functions available in the *Log* and *Tools* menus of the Web interface. These functions allow you to monitor and manage your Firewall.
- [Chapter 7](#) — [“Setting a Policy”](#) on [page 113](#) describes the functions available in the *Policy* menu of the Web interface. These functions enable you to control the traffic through your Firewall.
- [Chapter 8](#) — [“Advanced Settings”](#) on [page 137](#) describes the functions available in the *Advanced* menu of the Web interface. These functions enable you to configure your Firewall for different topologies of network and to provide some of the functionality of a router within your network.
- [Chapter 9](#) — [“Configuring Virtual Private Network Services”](#) on [page 151](#) describes the functions available in the *VPN* menu of the Web interface. These functions enable you encrypt and authenticate external access to your Firewall.
- [Chapter 10](#) — [“Configuring High Availability”](#) on [page 179](#) describes the functions available in the *High Availability* menu of the Web interface. These functions allow you to set up a second SuperStack 3 Firewall as a live backup should your Firewall fail.

Examining the Unit Status

To display the Firewall Unit Status, click *General* and click the *Unit Status* tab. A window similar to that shown in [Figure 21](#) displays.

Figure 21 Unit Status Window



This window shows the following information for your Firewall:

- Firewall Serial Number
- MAC Address
- Registration Code (once registered)
- ROM Version
- Firmware Version
- Device Up-time in days, hours, minutes, and seconds

Problems appear in red text. For example, if the Internet router was not contacted, or the default password was not changed, this would be listed. Items listed in red require immediate, corrective action. General operation status messages, such as enabled hacker attack protection, filter list status, and log settings are listed in black text.

Configuring the Administrator

From the *General* screen, select *Administrator*. A window similar to that in [Figure 22](#) displays.

Figure 22 Administrator Screen

Administrator login name

The default login for the administrator is *admin*. You can change this to prevent unauthorized access to the Web interface.



CAUTION: If the administrator login name is forgotten, you must reset the Firewall. See [“Resetting the Firewall”](#) on [page 198](#).

Change the Administrator Password

If you are setting the password for the first time, the default password is *password*. Change the administrator password to keep the Firewall secure.

- 1 In the *Old Password* box, type the old password.
- 2 In the *New Password* and *Confirm New Password* boxes type the new password
- 3 Click *Update* to save the new password.

The password cannot be recovered if it is lost or forgotten.



CAUTION: If the administrator password is forgotten, you must restore the Firewall to factory defaults. See [“Resetting the Firewall”](#) on [page 198](#).

Administrator Inactivity Timeout

The Administrator Inactivity Timeout option allows you to extend or reduce the period of time before the administrator is automatically logged out of the Web interface. The Firewall is pre-configured to logout the administrator after 5 minutes of inactivity.



The Firewall supports only one management session. If you login to the Firewall from a second Management Station, the first session is automatically logged out.

**Administrator and
User Login Failure
Handling**

You can prevent unauthorized attempts to access the Firewall by locking out users who fail to correctly login within a defined time period. Check the *Enable user lockout on login failure* box and then set the following parameters.

Lock out user after x failed login attempts in a 1 minute period

Set the number of failed login attempts allowed within a one minute period. The default is 5. The minimum is 1 and the maximum 99.

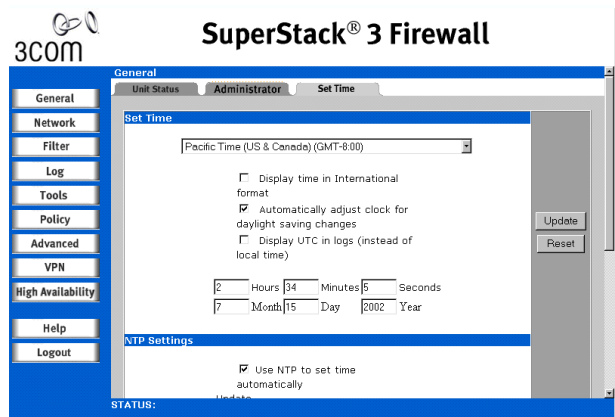
Lock out user for x minutes

Set the time period for which the user is locked out of the Firewall. The default is 5 minutes. The minimum is 0 (no lockout) and the maximum is 60 minutes.

Setting the Time

From the *General* menu, select *Set Time*. A window similar to that in [Figure 23](#) displays. This window allows you to set the date and time manually or to configure the Firewall to use NTP (Network Time Protocol) servers to set the time and date automatically.

Figure 23 Set Time Window



Set Time and Date Time Zone

Select your time zone from the drop-down list box at the top of the screen. If you cannot find your time zone in the list, you should set this to the one with the same offset from GMT as is used at your location.

Display Time in International Format

Displays the time and date in dd/mm/yy format instead of mm/dd/yy format.

Automatically adjust clock for daylight savings changes

Check this box to enable the Firewall to adjust to Daylight Savings Time automatically depending on the time zone you have chosen. This feature works with NTP on or off.

Display UTC (Universal Time) in logs instead of local time

Check this box to set the time on the Firewall to Universal Time Co-ordinated (UTC) time. UTC is the standard time common to all places in the world. It is also commonly referred to as Greenwich Mean Time or World Time. Many ISPs require firewall logs to be recorded in UTC as tracking hackers can be very difficult if reports of times are not consistent.

Manual Time Set

To set the time manually enter the date and time in the boxes at the bottom of the screen. Set the time in 24-hour clock, and use four digits to specify the year (for example, 2002).

NTP Configuration

You can configure the Firewall to use an NTP (Network Time Protocol) server to set the date and time.

Use NTP to set time automatically

Check this box to allow the Firewall to synchronize its time using an Network Time Protocol (NTP) server every hour. For example, if you started the Firewall at 2:30, the clock synchronizes every hour at the half hour—3:30, 4:30 etc.



To set the time automatically you need a connection to the Internet. 3Com recommends that initially you set the time manually even if you have selected this option.

See Manual Time Set above to set the time manually.

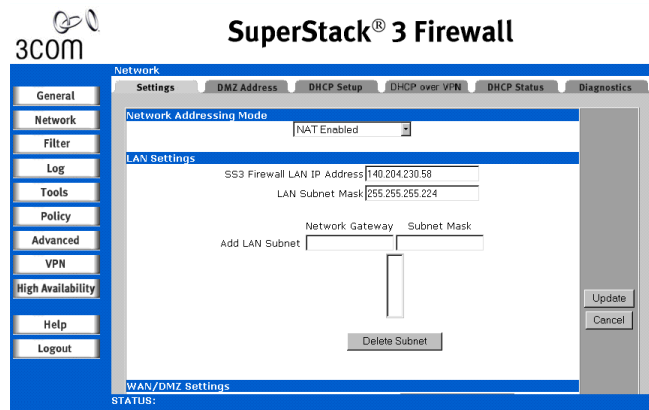
You can add NTP server addresses to the list to determine which NTP server the Firewall should use. Enter the IP address or NTP server address

in the *Add NTP Server* box. The Firewall uses the first NTP server in the list by default. If this is not available, it tries the next server in the list. If no servers are available, the Firewall uses its own internal NTP server list.

Changing the Basic Network Settings

Click *Settings* from the *Network* menu to display the *Network Settings* window shown in [Figure 24](#).

Figure 24 Network Settings Window



Setting the Network Addressing Mode

The *Network Addressing Mode* drop-down list contains five modes:

Standard

Choose *Standard* if you have IP addresses allocated by your ISP for each machine that requires access to the Internet. When you select *Standard*, Network Address Translation (NAT) is disabled. All nodes on the LAN must use a valid public IP address.

NAT Enabled

Choose *NAT Enabled* if you want to use a single IP address for accessing the Internet, or if you do not have an IP address allocated by your ISP for each machine that requires access to the Internet. NAT provides anonymity to machines on the LAN by connecting the entire network to the Internet using a single IP address. This is useful for two purposes:

- Additional security is provided because all the addresses on the LAN are invisible to the outside world.

- In cases where a network uses invalid IP addresses or if addresses are in short supply, NAT can be used to connect the LAN to the Internet without changing the IP addresses of computers and other devices on the LAN.



Remote authenticated access is not possible with NAT enabled.

When using IP addresses on a LAN which have not been assigned by an Internet Service Provider, it is a good idea to use addresses from a special address range allocated for this purpose. The following IP address ranges can be used for private IP networks and do not get routed on the Internet:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Select *NAT Enabled* from the *Network Addressing Mode* drop-down list if the network uses private IP addresses or if addresses are in short supply.

NAT with DHCP Client

Choose *NAT with DHCP Client* if you obtain the Firewall WAN IP address automatically from the Internet access device. If your ISP provided this device, confirm the IP address with your ISP.

NAT with PPPoE Client

Choose *NAT with PPPoE Client* if your Internet connection for the Firewall WAN IP Address is to be obtained from a remote PPPoE server.

NAT with L2TP Client

Choose *NAT with L2TP* if the WAN IP Address is obtained over the Internet using an L2TP connection.

Specifying the LAN Settings

For the LAN settings, specify:

Firewall LAN IP Address.

This is the IP address that is given to the Internet Firewall and used to access it for configuration and monitoring. Choose a unique IP address from the LAN address range.

LAN Subnet Mask

This value is used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address.

For example, consider the IP address 192.168.228.17. Assuming a Class C subnet mask of 255.255.255.0 is used, the first three numbers (192.168.228.) represent the Class C network address, and the last number (17) identifies a particular host on this network.

The following setting is also available if PPPoE is selected:

Connect/Disconnect

Click *Connect* in the Network Addressing Mode Section to initiate a PPPoE session. If all fields have been entered correctly, the Firewall connects to the Internet. You can terminate a PPPoE session by clicking *Disconnect*.

Add LAN Subnet

If your original LAN subnet is full and you need to add a new subnet without using a LAN router, you can configure the Firewall to recognize new subnets. Before you can configure multiple LAN subnets, you must have the following information:

- Network Gateway Address — This is an IP address assigned to the Firewall in addition to the existing LAN port IP address. If you have configured the Firewall in Standard mode, the IP address should be the Default Gateway IP address assigned to your Internet router on the same subnet. All users on the subnet you are configuring must use this IP address as their default router/gateway address.
- Subnet Mask — This value defines the size and scope of the subnet based upon the Network Gateway entry. If you are configuring a subnet mask that currently exists on the LAN port, enter the existing subnet mask in this field. If you are configuring a new subnet mask, use a subnet mask that does not overlap any previously defined subnet masks.



The Firewall cannot be managed from any of the additional Network Gateway addresses. You must use the IP address for the LAN port to manage the Firewall. Also you cannot mix Standard and NAT subnets behind the Firewall.



This feature does not replace adding static routes for reaching subnets on the other side of a router. Use the Advanced > Static Routes option to do this.

Specifying the WAN/DMZ Settings

For the WAN/DMZ settings, specify:

WAN Gateway (Router) Address

The WAN gateway address, also called the default gateway, is the address of the router that attaches the LAN to the Internet.

Firewall WAN IP Address

This value is automatically set except in *NAT enabled* mode for the Firewall. For *NAT Enabled* mode enter the value specified by your ISP.

WAN/DMZ Subnet Mask

This value is automatically set for the Firewall except in *NAT enabled* mode. For *NAT Enabled* mode enter the value specified by your ISP.

If PPPoE is selected, you also have to set the following:

User Name

Enter the *User Name* for your PPPoE account in this section. This is information given to you by your service provider upon initial installation of your broadband service.

Password

Enter the *Password* for your PPPoE account in this section. This is information given to you by your service provider upon initial installation of your broadband service.

Gateway (Router) Address:

This address is provided automatically by your service provider.

L2TP Settings

This setting is only used if your ISP connection uses L2TP. Separate configuration parameters are used to configure VPN connections using L2TP

For more information about PPPoE refer to ["Frequently Asked Questions about PPPoE"](#) on [page 203](#).

Specifying the DNS Settings

In the *DNS Settings* section, specify the *DNS Servers*. Up to three DNS servers can be specified, although not all have to be used. The Firewall uses these servers to look up the addresses of machines used to download the Web Site Filter and for the built-in *DNS Lookup* tool.

Type the required values and click *Update* to save the changes. It is necessary to restart the Firewall for these changes to take effect.

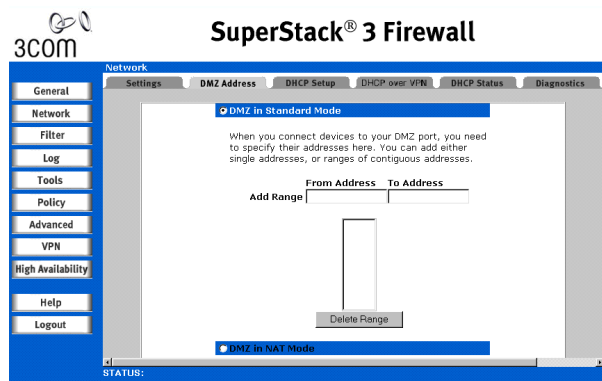
Specifying DMZ Addresses

The Firewall provides security by preventing Internet users from accessing machines inside the LAN. This security, however, also prevents users from reaching servers intended for public access, such as a Web or e-mail server, which are crucial for effective Internet use.

In order to allow such services, the Firewall comes with a special *Demilitarized Zone* (DMZ) port which you use for setting up public servers. The DMZ is located between the local network and the Internet. Servers on the DMZ are publicly accessible, but they are protected from attacks such as SYN Flooding and Ping of Death. Use of the DMZ port is optional and you do not have to connect it.

Click *Network*, and then select the *DMZ Addresses* tab. A window similar to that in [Figure 25](#) displays.

Figure 25 DMZ Address Window



DMZ in Standard Mode

Type the addresses for the DMZ individually or as a range. Type an individual address in the *From Address* box. To enter a range of addresses, such as the IP addresses from 199.168.23.50 to 199.168.23.100, type

the starting address in the *From Address* box and the ending address in the *To Address* box. You can specify up to 64 address ranges.



Each of the servers on the DMZ needs a public IP address. Obtain these IP addresses from your ISP. Usually, the ISP can also supply information on setting up public Internet servers.

Click *Update* to save your changes.

To delete an address or range, select it in the *Address Range* list and click *Delete Range*.

DMZ in NAT Mode

The Firewall *DMZ* now has the ability to use private internal IP addresses rather than public IP addresses on the network. Since NAT hides the true IP addresses in use on the network, NAT on the DMZ is an additional security feature for the Firewall. The outside world only sees the outside public IP address of the DMZ and not the internal private addresses.

The ability to run the DMZ port in NAT mode, not only provides additional security for publicly accessible servers, it can also be used to configure an additional security zone, for example in education establishments where you may want to have a teacher / administration network, separated from a student network, in this example the teacher / administration network is attached to the DMZ port, with the student network attached to the LAN port. Here both networks are protected against threats from the outside world through the WAN port, but at the same time the teacher / administrator network can be configured to provide protection from the student network as well.

To configure the *DMZ in NAT Mode*, carry out the following:

- 1** In the *DMZ Private Address* field, enter the private internal IP address assigned to the DMZ interface.
- 2** Assign a subnet mask in the *DMZ Subnet Mask* field. The LAN and DMZ can have the same subnet mask, but the subnets must be different. For instance, the LAN subnet can be 192.168.0.1 with a subnet mask of 255.255.255.0, and the DMZ subnet can be 172.16.18.1 with a subnet mask of 255.255.255.0.
- 3** If you choose to use *DMZ NAT Many to One Public Address (Optional)*, enter the DMZ public IP address which is on the same subnet as the WAN for access to devices on the DMZ interface. *DMZ NAT Many to One Public*

Address is only available if your Firewall is configured in *NAT Enabled* networking mode.

Setting up the DHCP Server

Dynamic Host Configuration Protocol (DHCP), is a means for computers on a network to obtain their IP settings from a centralized server.

DHCP offers complete centralized management of IP client configurations, including IP addresses, gateway address, and DNS address.



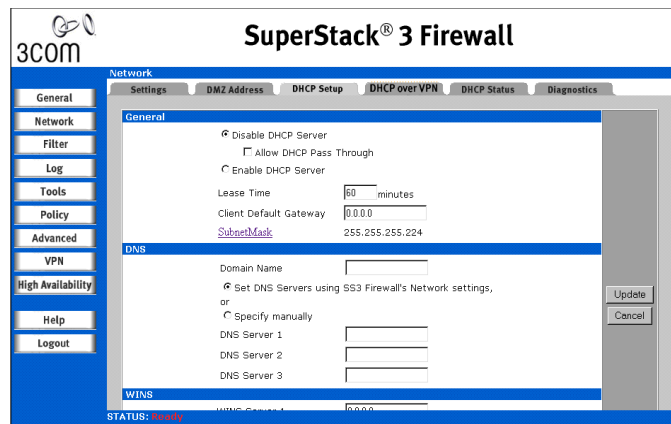
See [“Dynamic Host Configuration Protocol \(DHCP\)” on page 219](#) for more information about DHCP.



The Firewall can allocate up to 255 static or dynamic IP addresses. 3Com recommends you use a dedicated DHCP server if more addresses are required.

To set up the DHCP server on the Firewall click *Network*, and then click *DHCP Server*. A window similar to that in [Figure 26](#) displays.

Figure 26 DHCP Setup Window



Global Options Disable/Enable DHCP Server

Click the appropriate radio button to enable or disable the DHCP server. This is disabled by default. Leave the DHCP server disabled if there already is a DHCP server on the LAN or if manual addressing is used on the LAN computers.

Enable DHCP PassThrough

Check this box if you obtain IP addresses from a DHCP server connected to the WAN port of the Firewall. For example, your Internet access device.

Lease Time

This is the amount of time that the IP address is leased, or given to the client machine before the DHCP server attempts to renew that address. If the client still requires the use of the IP address, the DHCP Server grants the client the use of that IP address for the same amount of time. If the client no longer requires the IP address, the address is freed and returned to the pool of available addresses to be used again. The default value is 60 minutes.

Client Default Gateway

Enter the IP address of the WAN router used by LAN clients to access the Internet. If NAT is being used this is the LAN IP address of the Firewall.

Subnet Mask

Enter the Subnet mask for your network. This value is given out by the DHCP server and is used by client devices to determine the extent of your network.

Domain Name

Type the registered domain name for the network in the *Domain Name* box, for example: **3com.com**. If you do not have a Domain Name leave this blank.

DNS Servers

A DNS Server translates human readable host names into the numeric IP addresses used by computers to route information to the correct machine. You can use multiple DNS servers to improve performance and reliability. To specify these manually select the *Specify Manually* radio button and type the IP address of the DNS Server(s) in these boxes.

Alternatively, if you are using NAT with DHCP client you can select the *Set DNS Servers by Internet Firewalls DHCP Client* to have these fields set automatically.

Dynamic Ranges

When a client makes a request for an IP address, the Firewall's DHCP server leases an address from the Dynamic Ranges.



Prior to offering an address from the Dynamic Range to a requesting client, the Firewall first verifies that the address is not already in use by another machine on the LAN.

To create a range of dynamic IP addresses to be assigned to requesting clients, type the starting number in the *Range Start* box, the ending address in the *Range End* box and then click *Update*.

Allow BootP clients to use range

Click this check box to have Dynamic BootP clients configured when they boot. Dynamic BootP clients are BootP clients that do not have an IP address assigned to their MAC address. They are similar to DHCP clients with the exception that leases are not supported.

Delete Range

To remove a range of addresses from the dynamic pool, select it from the scrolling list of dynamic ranges, and click *Delete Range*.

Static Entries

Static addresses are used by client machines that support BootP or those which require a fixed IP address. For example, client machines running Web or FTP servers require static addresses.

To create a static IP address to be assigned to a requesting client, type an IP address and the Ethernet (MAC) address of the client machine in the appropriate boxes and click *Update*.

Delete Static

To remove a static address, select it from the scrolling list of static addresses and click *Delete Static*.

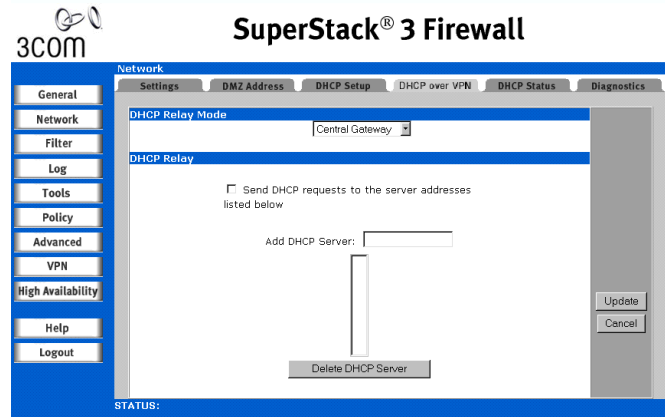
Setting up DHCP over VPN

DHCP over VPN allows a PC (DHCP Client) behind a Firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.

You need to configure the Firewalls at the remote and central site for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The Firewall at the remote site must be configured as a *Remote Gateway* to pass DHCP broadcast packets through its VPN tunnel. The

Firewall at the central site must be configured as a *Central Gateway* to relay DHCP packets from the client on the remote network to the DHCP server on the central site.

Figure 27 DHCP over VPN Window



Configuring a Central Gateway

To configure DHCP over VPN as the *Central Gateway*, carry out the following:

- 1 Log into the Management interface, click *Network*, and then select *DHCP over VPN*. A window similar to that in [Figure 27](#) displays
- 2 Select *Central Gateway* from the DHCP Relay Mode drop-down list.
- 3 If you want to send DHCP requests to specific servers, enable the *Send DHCP requests to the server addresses listed below* check box.
- 4 Type the IP addresses of DHCP servers in the *Add DHCP Server* field, and click *Update*. The Firewall now directs DHCP requests to the specified servers.
- 5 To delete DHCP servers, click on the IP address of the DHCP server, and click *Delete DHCP Server*. The server is removed from the list of DHCP servers.
- 6 To complete the configuration, go to *VPN* and click *Configure*. Select *Destination network obtains IP addresses using DHCP through this SA* in the *Destination Networks* section. Click *Update*.

To delete a lease in order to free the IP address in the DHCP server, select the lease from the list and then click *Delete Lease*. The transmit operation

takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click *Refresh* to reload the list of leases. This may be necessary because Web pages are not automatically refreshed and new leases may have been issued since the page was first loaded.

Configuring a Remote Gateway

To configure the Firewall as a *Remote Gateway*, carry out the following:

- 1 Log into the Management interface, click *Network*, and then *DHCP over VPN*.
- 2 Select *Remote Gateway* from the *DHCP Relay Mode* menu.
The screen changes to show the *LAN IP Addresses* and *LAN Device Configuration* sections.
- 3 Enter the *LAN IP Addresses*.
 - a Select the VPN Security Association to be used for the VPN tunnel from the *Obtain using DHCP through this SA* menu.



Only VPN Security Associations using IKE can be used as VPN tunnels for DHCP.

- b The *Relay IP address* determines the IP addresses in the central DHCP server to be distributed to the Firewall's LAN. It must be in the same DHCP scope as the central IP address pool but excluded from distribution.
- c If you enable *Block traffic through tunnel when IP spoof detected*, the Firewall blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is entered for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the Firewall to respond to IP spoofs.
- d If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Check the *Obtain temporary lease from local DHCP server if tunnel is down* box. By checking this box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, enter the number of minutes for the temporary lease in the *Temporary Lease Time* box. The default value is two (2) minutes.

4 Enter the *LAN Device Configuration* details.

- a** To configure *Static Devices on the LAN*, enter the IP address of the device in the *IP Address* field.
- b** Then enter the Ethernet Address of the device in the *Ethernet Address* field.

An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have *Block traffic through tunnel when IP spoof detected* enabled, it is not necessary to enter the Ethernet address of a device.



You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients.

- c** Select *LAN Devices not allowed to obtain IP through SA* if there are devices on the LAN that you do not want to obtain IP addresses through the VPN tunnel, such as children's computers. You must know the Ethernet address of the device to configure this setting. The Ethernet address of a device can be determined by typing **winipcfg** for Windows 98 systems or **ipconfig/all** for Windows XP or Windows 2000 systems into a Command Prompt window.



You must configure the local DHCP server on the remote Firewall to assign IP leases to these computers.



If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote PC.

Viewing the DHCP Server Status

Click *Network* and then select the *DHCP Server Status* tab. A window similar to that in displays.

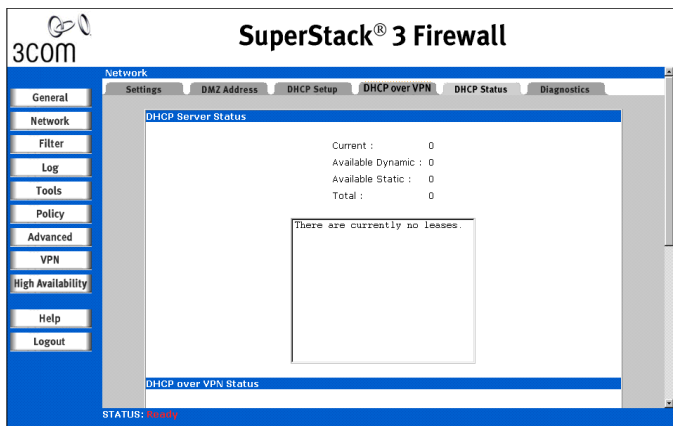
DHCP Server Status

The scrolling window shows the details on the current bindings:

- IP and MAC address of the bindings
- Type of binding (Dynamic, Dynamic BootP, or Static BootP).

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list and then click *Delete*.

Figure 28 DHCP Status Window



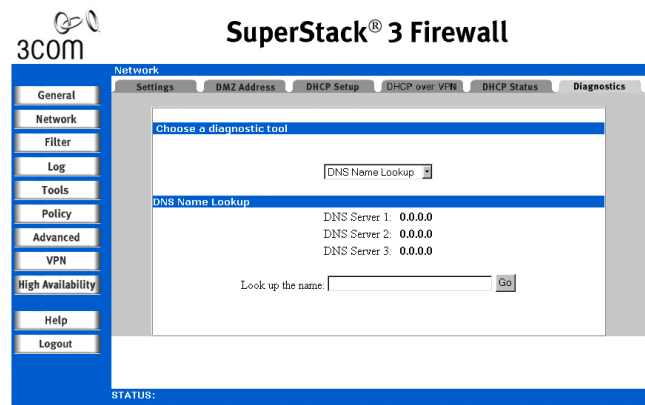
DHCP over VPN Status

This section reports the number of *Current Dynamic*, Current Static, and the *Total leases*. The scrolling window shows the current static and dynamic hosts behind the Remote Gateway. The IP address, MAC address, and lease expiration are shown. On Central Gateways, the VPN tunnel of the remote host is also displayed. Take care when deleting entries from the table, deleted hosts do not have access to the tunnel once deleted.

Using the Network Diagnostic Tools

The Firewall has several tools built in which can help you solve network problems. Click *Network*, and then select the *Diagnostics* tab.

Figure 29 Diagnostics Window



Choosing a Diagnostic Tool

The drop-down box provides six diagnostic tools:

DNS Name Lookup

Domain Name Service (DNS) is an internet service which allows users to enter an easily remembered host name, such as `www.3Com.com`, instead of numerical IP addresses to access Internet resources. The Firewall has a *DNS Lookup* tool that returns the numerical IP address of a host name.

- 1 Select *DNS Name Lookup* from the *Choose a diagnostic tool* menu.
- 2 Type the host name to lookup in the *Look up the name* box and click *Go*. The Firewall then queries the DNS server and displays the result at the bottom of the screen.



The IP address of at least one DNS Server must be present on the Network Settings tab for the DNS Name Lookup feature to function.

Find Network Path

Use the *Find Network Path* tool to show on which port, LAN, WAN or DMZ where appropriate, an IP host is located. This is helpful to determine if the Firewall is properly configured. For example, if the Firewall *thinks* that a machine known to be on the Internet is located on the LAN port, then there is a problem with the configuration of the network or intranet settings. *Find Network Path* also shows if the target node is behind a

router, and the Ethernet address of the target node or router. *Find Network Path* also shows which router a node is using, which can help isolate router configuration problems.

- 1 Select *Find Network Path* from the *Choose a diagnostic tool* menu.
- 2 Type the IP address of the device and click *Go*. The test takes a few seconds to complete.

If the network path is incorrect, check the intranet, static route, DMZ and VPN settings.

Find Network Path requires an IP address. Use the Firewall's DNS Name Lookup tool to find the IP address of a host.

Ping

The *Ping* tool bounces a packet off a machine on the Internet back to the sender. This test shows if the Firewall is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or other machine at the ISP's location. If this test is successful, try pinging devices outside the ISP. This shows if the problem lies with the ISP's connection.

- 1 Select *Ping* from the *Choose a diagnostic tool* menu.
- 2 Type the IP address or host name of the device being pinged and click *Go*. The test takes a few seconds to complete.

Packet Trace

Use the *Packet Trace* tool to track the status of a data packet or communications stream as it moves from source to destination. This is a useful tool to determine if a packet or communications stream is being stopped at the Firewall, or is lost on the Internet.

Select *Packet Trace* from the *Choose a diagnostic tool* drop-down list.



Packet Trace requires an IP address. Use the Firewall's DNS Name Lookup tool to find the IP address of a host.

- 1 Enter the IP address of the remote host in the *Trace on IP address* box, and click *Start*.
- 2 Initiate an IP session with the remote host using an IP client, such as Web, FTP, or Telnet.

Use the IP address in the *Trace on IP address* box, not a host name, such as `www.3Com.com`.

- 3 Click *Refresh* to display the packet trace information.
- 4 Click *Stop* to terminate the packet trace, and *Reset* to clear the results.

Technical Support Report

The *Tech Support Report* generates a detailed report of the Firewall's configuration and status, and saves it to the local hard disk. You can then e-mail this file to Technical Support to help assist with a problem.

- 1 Select *Tech Support Report* from the *Choose a diagnostic tool* menu.
- 2 Enable the required report options.
- 3 Click *Save Report* to save the report as a text file to the local disk.

Trace Route

Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, Trace Route can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds. Enter the IP address or domain name of the destination host. For example, enter **yahoo.com** and click *Go*. A second window is displayed with each hop to the destination host. By following the route, you can diagnose where the connection fails between the Firewall and the destination.

5

SETTING UP WEB FILTERING

This chapter describes the commands and options available in the *Filter* menu. The menu is broken up into four sections shown in the user interface as tabs.

To access a command click *Filter* and then on the appropriate tab.

The following sections are covered in this chapter:

- [Configuring the Filtering Options](#)
- [Configuring the URL List](#)
- [Customizing the 3Com Web Filter](#)
- [Filtering by User Consent](#)
- [Configuring the Firewall for use with N2H2](#)
- [Configuring the Firewall for use with Websense Enterprise](#)

See [Chapter 11](#) for background information about web filtering.

Configuring the Filtering Options

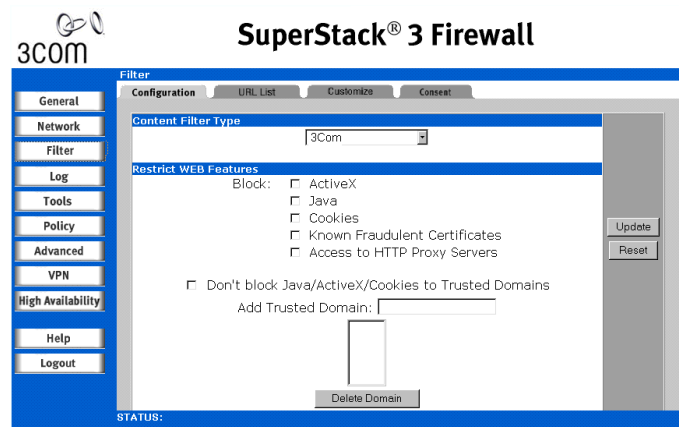
The Firewall supports the following filtering options:

- Manual Filtering
- 3Com Content Filtering (subscription service)
- Third Party Content Filtering

Content Filtering only applies to nodes on the LAN Port. Click *Filter*, and then the *Configure* tab. A window similar to that in [Figure 30](#) displays.



For more information about the 3Com Website Filter, see [“Introducing the Web Site Filter”](#) on [page 189](#)

Figure 30 Filter Settings Window

Content Filtering Use the drop-down menu to select the type of filtering you wish to use. The options are:

3Com

Select this option if:

- You wish to use the Firewall's Internet manual filtering option. This option lets you configure the URL list and completely customize your Content Filter feature. It includes allowed and forbidden domains and filtering used keywords.
- You subscribe to 3Com's web filtering service. Note that one month's subscription is provided free of charge when you register your Firewall.



You may combine manual filtering with 3Com's web filtering service. However, you cannot combine manual filtering with Third Party filtering options.

N2H2

N2H2 is a third party content filter package that is supported by the Firewall. You can obtain more information about N2H2 at <http://www.n2h2.com>. Select this option if you have subscribed to N2H2's service and want to configure access to the N2H2 server. If you select N2H2 from the list, an *N2H2* tab is available to configure the location of the N2H2 server and other settings. Customization of allowed and forbidden domains is available if you select N2H2. See ["Configuring the Firewall for use with N2H2"](#) on [page 91](#) for more information.

Websense Enterprise

Websense Enterprise is also a third party content filter package that is supported by the Firewall. You can obtain more information about Websense Enterprise at <http://www.websense.com>. Select this option if you have subscribed to Websense Enterprise's service and want to configure access to the Websense server. If you select Websense Enterprise, a *Websense* tab is available to configure the location of the Websense Server and other settings. Customization of allowed and forbidden domains is available if you select Websense. See [“Configuring the Firewall for use with Websense Enterprise”](#) on [page 93](#) for more information.



3Com cannot provide any support for third party filtering options. Please contact N2H2 or Websense as applicable or your supplier for support or technical advice.

Restricting the Web Features Available

The following is a list of the web features that you can control using the Web Filter. To allow your network to access a category leave the check box clear. To deny your network access to a category check the box corresponding to that category.

ActiveX

ActiveX is a programming language that is used to embed small programs in Web pages. It is generally considered an insecure protocol to allow into a network since it is possible for malicious programmers to write controls that can delete files, compromise security, or cause other damage.

Java

Java is also used to embed small programs, also called applets, in Web pages. It is generally considered safer than ActiveX since it has more thorough safety mechanisms. However, some administrators may choose to filter out Java since there have been instances of bugs in these safety mechanisms.

Cookies

Cookies are used by Web servers to track usage. Unfortunately, cookies can be programmed not only to identify the visitor to the site, but also to track that visitor's activities. Because they represent a potential loss of privacy, some administrators may choose to block cookies.

Known Fraudulent Certificates

Digital certificates help verify that Web content and files originated from an authorized party. If digital certificates are proven fraudulent, then the Firewall blocks Web content and files that use these fraudulent certificates. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates.

Access to HTTP Proxy Servers

When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. This feature disables access to proxy servers located on the WAN. It has no effect on those located on the LAN.

Using Trusted Domains

If you trust content on specific domains, you can select *Don't Block Java / Active X / Cookies to Trusted Domains* and then add the Trusted Domains to the firewall. Java scripts, Active X and cookies are not blocked from Trusted Domains if the box is checked. All content from trust domains is allowed through the Firewall.

Changing the Message to display when a site is blocked

When a user attempts to access a site that is blocked by the Web Site Filter, a message is displayed on their screen. The default message is:

```
Web Site Blocked by 3Com SuperStack 3 Firewall.
```

You can type any message, including embedded HTML, up to 255 characters long in this box.

For example, if you type the following:

```
Access to this site was denied because it appears to
violate this organization's
<A HREF=http://www.your-domain.com/acceptable_use_policy.htm>Acceptable Use Policy</A>. Please contact the
<A HREF="mailto:admin@your-domain.com">Network
Administrator</A> if you feel this was in error.
```

The user will see the following displayed when they attempt to visit a blocked site:

```
Access to this site was denied because it appears to
violate this organization's Acceptable Use Policy. Please
```

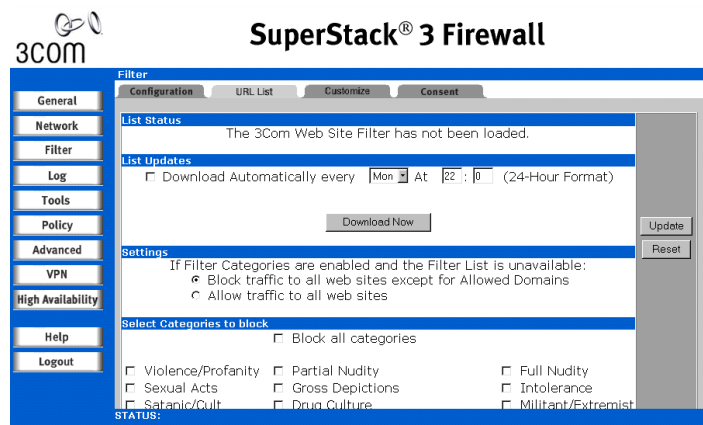
contact the Network Administrator if you feel this was in error.

Where the underlined sections are links to your company's acceptable use policy and to the network administrator's email address.

Configuring the URL List

Click *Filter*, and then select the *URL List* tab. A window similar to that in [Figure 31](#) displays.

Figure 31 URL List Window



Checking the Web Filter Status

This section shows the status of the Web Site Filter and the date it was last downloaded. If the Web Site Filter has not been downloaded the Firewall displays a warning message in red text.

Updating the Web Filter

Since content on the Internet is constantly changing, make sure you update the 3Com Web Site Filter used by the Firewall on a regular basis. When you subscribe to the Web Site Filter, you can specify that it is updated automatically every week for one year.

It is important to note that host names, and not IP addresses, are used for all Internet filtering functions. This is for two reasons:

- Many blocked sites operate server pools, where many machines service a single host name, making it impractical and difficult to add and maintain the numerical addresses of every server in the pool.

- Many sites included in the Web Site Filter regularly change the IP address of the server to try to bypass the Web Site Filters. This makes maintaining a current list subscription critical for effective content filtering.

Automatic Download

Check this box to enable automatic, weekly updates to the Web Site Filter. Also, select the day of the week and the time of the day to download the new list. A valid Web Site Filter subscription is required. It is recommended that you download the updates at a time of low Internet access to prevent disruption to the network.

Download Now

Click this button to download and update the Web Site Filter immediately. This process may take a couple of minutes, depending on Internet traffic conditions and requires a valid subscription to the Web Site Filter.

Setting Actions if no Filter List is Loaded

There are two radio buttons that determine what happens if the Filter List expires or if a download of a Filter List fails:

Block traffic to all websites except for Trusted Domains

Select this option if only access to Trusted Domains should be available in the event of the Filter List expiring or a download failing. See [“Setting up Trusted and Forbidden Domains”](#) on [page 86](#) for more information.

Allow traffic to all websites

Select this option to provide open access to the Internet in the event of the Filter List expiring or a download failing.



Since it is necessary to restart the Firewall once the download is complete, which causes a momentary interruption of Internet access, it is a good idea to download new lists when LAN access to the Internet is at a minimum.

Click *Update* to save your changes.

Once loaded, the creation date of the current active list is displayed.



Each download of the Web Site Filter expires 30 days after it is downloaded. The Filter List may also be erased if the Firewall fails to

download a new list. If the Filter List expires or is erased, the Firewall may be configured to block all Web Sites except for Trusted Domains, or to allow access to all Web Sites.

Specifying the Categories to Filter

The Web Site Filter can control access from the LAN to thousands of Web sites that might be deemed inappropriate for your organization. Twelve selectable Web site categories are provided so Internet access can be tailored to the needs of the organization. Check the boxes for those categories you wish to block. See ["Introducing the Web Site Filter"](#) on [page 189](#) for a detailed explanation.

- Violence/Profanity
- Partial Nudity
- Full Nudity
- Sexual Acts
- Gross Depictions
- Intolerance
- Satanic/Cult
- Drugs/Drug Culture
- Militant/Extremist
- Sex Education
- Questionable/Illegal & Gambling
- Alcohol & Tobacco

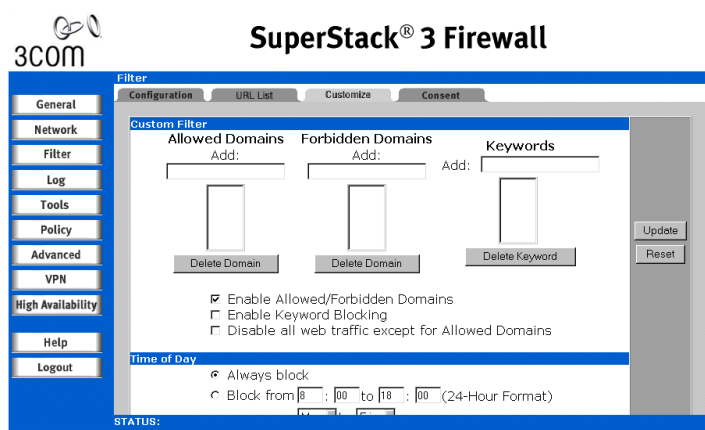


To check the listing of a site or to submit a new site, go to the Firewall's Web page at <http://www.3com.com/ssfirewall> and follow the on-screen instructions.

Customizing the 3Com Web Filter

This function allows you to block specific web sites, or restrict access to a list of approved web sites if you have selected the 3Com option for your *Content Filter*. This is in addition to the Web Site Filter and overrides the more general Web Site Filter categories.

Click *Filter*, and then select the *Custom List* tab. A window similar to that in [Figure 32](#) displays.

Figure 32 Customize Window

Setting up Trusted and Forbidden Domains

You can add or remove web sites from the Custom List. For example, if a local radio station runs a contest on its Web site that is disrupting normal classroom Internet use, a school's Technology Coordinator can easily add that site to the *Forbidden Domains* list.

Trusted Domains — To allow access to a Web site which has been blocked by the Web Site Filter, type its host name, such as **www.ok-site.com**, into the *Trusted Domains* box. Do not use the complete URL of the site, that is, do not include **http://**. All subdomains are allowed. For example, adding **3Com.com** also allows **www.3Com.com**, **my.support.3com.com**, **shop.3com.com** and so forth. Up to 256 entries are supported in the *Trusted Domains* list. Click *Update* to send the update to the Firewall.

Forbidden Domains — To block a Web site which has not been blocked by the Web Site Filter, type its host name, such as **www.bad-site.com** into the *Forbidden Domains* box. Do not use the complete URL of the site, that is, do not include **http://**. All subdomains are blocked. For example, adding **bad-site.com** also blocks **www.bad-site.com**, **my.support.bad-site.com**, **shop.bad-site.com** and so forth. Click *Update* to save your changes.

To remove a site which was previously added, select its name in the list box, and click *Delete Domain* to send the update to the Firewall.

Enable Allowed/Forbidden domains

To activate the Allowed and Forbidden domains, make sure you check the *Enable Allowed/Forbidden domains* check box.

Disable all Web traffic except for Trusted Domains

Click the *Disable Web traffic except for Trusted Domains* check box to allow Firewall Web access only to sites on the *Trusted Domains* list. With careful screening, this can block almost all objectionable material.

Using Keyword Filtering

You can block Web URLs that contain specified keywords. This functions as a second line of defense against objectionable material. For example, if you specify the keyword **xxx**, the following URL:

`http://www.new-site.com/xxx.html`

is blocked, even if it is not included in the Web Site Filter.



It is important to use caution when enabling this feature. For example, blocking the word breast may stop access to sites on breast cancer as well as objectionable or pornographic sites.

To enable this function check the *Enable Keyword Blocking* check box and click *Update*.

To add a keyword, in the *Add Keyword* box, type the keyword to block and click *Update*.

To remove a keyword, select it from the list and click *Delete Keyword*.

Enable Keyword Blocking

To activate keyword blocking, make sure you check the *Enable Keyword Blocking* check box.

Specifying When Filtering Applies

Use the *Time of Day* setting to define time periods during which Internet filtering is enabled. For example, in a school, it might be useful to enable Internet filtering during normal school hours to protect students, but to disable it after hours to give teachers complete access to the Internet. Similar policies could be enabled to allow employees complete access to the Internet after normal business hours.



Time of Day restrictions only apply to the Web Site Filter, Custom Sites, and Keywords. Consent and Restrict Web Features, such as ActiveX, Java, cookies and Web Proxy, are not affected.

Always Block

If you select this option, Internet Filtering is always active and Time of Day limitations are not enforced. This is enabled by default.

Block Between

If you select this option, Internet Filtering is only active during the time interval and days specified.

Enter the time period, in 24-hour format, and the start and end day of the week during which you want to enforce Internet Filtering.

Setting Blocking Options

There are two blocking options:

Log Only

If you select this option, the Firewall logs and then allows access to all sites on the Web Site Filter, custom, and keyword lists. Use this function to monitor inappropriate usage without restricting access.

Log and Block Access

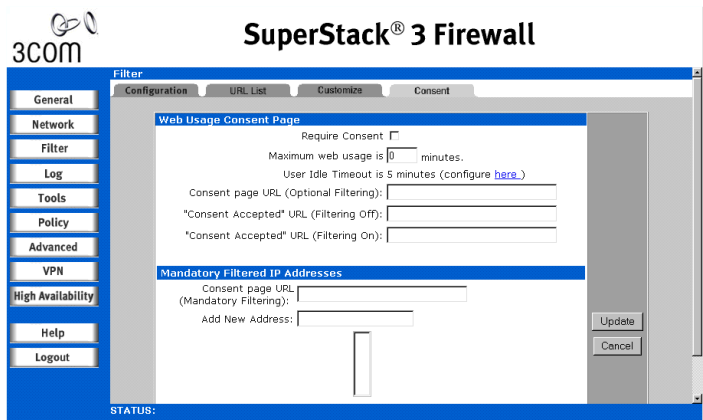
If you select this option, the Firewall logs and blocks access to all sites on the Web Site Filter, custom, and keyword lists.

Filtering by User Consent

Click *Consent* on the *Filter* menu to specify which computers are always filtered and which are filtered only when such protection is requested by the user. You can also configure *Consent* to require users to agree to the terms outlined in an organization's *Acceptable Use Policy* before you allow them to browse the Web any further.

Click *Filter*, and then *Consent*. A window similar to that in [Figure 33](#) displays.

Figure 33 Consent Window



Configuring User
Consent Settings

Require Consent

Check this box to enable the consent features.

Maximum web usage is

In an environment where there are more users than computers, such as a classroom or library, you can set a time limit on computer use. Type the time limit, in minutes, in the *Maximum web usage is* box. Specify the default value of zero (0) to disable this feature. If you set a limit, the Firewall reminds users when their time has expired by displaying the page defined in the *Consent page URL* box

User idle timeout

After a period of inactivity, the Firewall requires the user to agree to the terms outlined in the *Consent* tab before it allows any additional Web browsing. To configure the value, follow the link to the *User Privileges* window and type the desired value in the *Privileged User Idle Timeout* box.

Consent page URL (Optional Filtering)

When users begins an Internet session on a computer that is not always filtered, they are shown a consent page and given the option to access the Internet with or without filtering.

Create this page in HTML on a local Web server. It may contain the text from, or links to your company's *Acceptable Use Policy (AUP)*.

You must include in this page links to two pages contained in the Firewall which, when selected, tell the Firewall if the user wishes to have filtering enabled or disabled. The link for unfiltered access must be:

`192.168.1.254/iAccept.html`

The link for filtered access must be:

`192.168.1.254/iAcceptFilter.html`



If you have changed the IP address or the Firewall use the IP Address of the Firewall instead of 192.168.1.254.



Both the link for filtered access and the link for unfiltered access are case sensitive.

When entering the following addresses you should not enter `http://` before the address.

“Consent Accepted” URL (Filtering Off)

When users accept the terms outlined in the Consent page and choose to access the Internet without the protection of filtering, they are shown a page to confirm their selection. Type the URL of this page in the “*Consent Accepted*” URL (*Filtering Off*) box.

“Consent Accepted” URL (Filtering On)

When users accept the terms outlined in the Consent page and choose to access the Internet with the protection of filtering, they are shown a page to confirm their selection. Type the URL of this page in the “*Consent Accepted*” URL (*Filtering On*) box.

Mandatory Filtered IP Addresses

When users begin an Internet session on a computer where filtering is mandatory, as described below, they are shown a consent page. You create this page, and can add the text from the Acceptable Use Policy (AUP), and notification that violations of the AUP are blocked and logged.

Consent Page URL (Mandatory Filtering)

When users access a page that you include in the list of Mandatory Filtered IP Addresses the user is shown a page to inform them that the page is Filtered. Type the URL of this page in the *Consent page URL (Mandatory Filtering)* field.

You must include a link in this page to:

`192.168.1.254/iAcceptFilter.html`



If you have changed the IP address or the Firewall use the IP Address of the Firewall instead of 192.168.1.254.



Click Update to save your changes.



The link for filtered access is case sensitive.

Add New Address

You can configure the Firewall to provide filtering always for certain computers on the LAN. Type the IP addresses of these computers in the *Add New Address* box and click *Submit*. You can add up to 128 IP addresses. To remove a computer from the list of computers to be filtered, highlight the IP address in the list and click *Delete Address*.



To filter individual users by IP address you must use static IP addressing.

Configuring the Firewall for use with N2H2

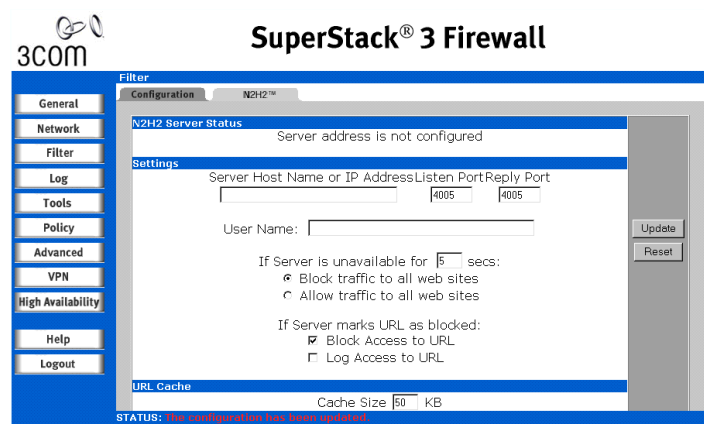
If you have opted to use N2H2 as the source for your Content Filter List, you should refer to your N2H2 documentation for details of configuring N2H2 Internet Filtering for your network.



3Com cannot provide any support for N2H2. Please contact N2H2 or your supplier for support or technical advice.

If you select *N2H2* in the *Configuration* tab, the tab options change. Select *N2H2* to view the screen displayed in [Figure 34](#).

Figure 34 N2H2 Window



N2H2 Status This section displays the status of the N2H2 Internet Filtering Protocol (IFP) server you are using for Internet Filtering.

Settings This section allows you to configure the Firewall to work with an N2H2 server.

Server Host Name or IP Address

Enter the Server Host Name or the IP address of the N2H2 Internet Filtering Protocol (IFP) server used to receive IFP requests.

Listen Port

Enter the UDP port number for the N2H2 IFP server to listen for the N2H2 traffic. The default port is 4005.

Reply Port

Enter the UCP port number for the N2H2 server to send packets from the N2H2 client to the Firewall. The default port is 4005.

User Name

The User Name refers to a configuration of users, a group of users or network defined in the N2H2 software.

If Server is unavailable for 5 secs

The default value for timeout of the server is 5 seconds but you can enter a value of between 1 and 10 seconds. If the N2H2 server becomes unavailable, select one of the following:

- *Block traffic to all websites*
- *Allow traffic to all websites*

If Server marks URL as blocked

If the server marks the URL as blocked you can select one of following actions for the Firewall:

- *Block Access to the URL*
- *Log Access to the URL*

URL Cache You can configure the *URL Cache* in KB. A larger *URL Cache* can provide noticeable improvements in Internet browsing response times.

Configuring the Firewall for use with Websense Enterprise

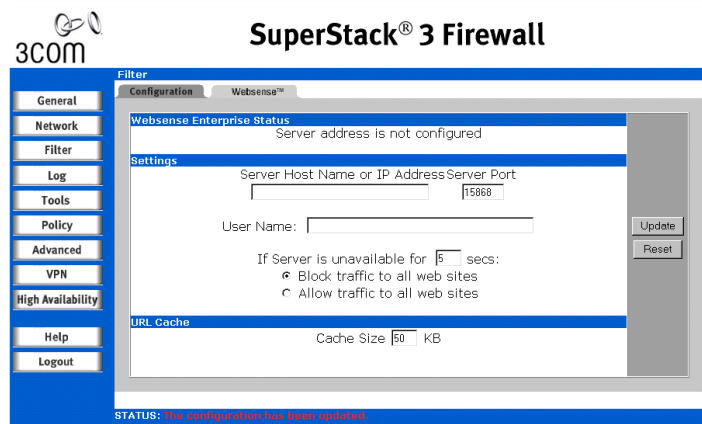


Websense is a third party software package that allows you to use content filtering through the Firewall. Customization of the Content Filter List is not available if you select Websense as your source for content filtering.

3Com cannot provide any support for Websense Enterprise. Please contact Websense or your supplier for support or technical advice.

If you select *Websense Enterprise* in the *Configure* tab, the tab options change. Select *Websense* to view the screen displayed in [Figure 35](#).

Figure 35 Websense Window



Websense Server Status

This section displays the status of the Websense Enterprise server used for content filtering.

Settings

Server Host Name or IP Address

Enter the Server Host Name or IP address of the Websense Enterprise server used for the content filter list.

Server Port

Enter the UDP port number for the Firewall to listen for the Websense Enterprise traffic. The default port is 15686.

User Name

Leave this field blank to enable reporting for users and groups defined on the Websense Enterprise server. Enter a *User Name* configured on the

Websense Enterprise Server for a user or a group to provide specific reporting on a user or group of users.

If you are using NT-based directories on the Websense Enterprise server, the user name is in the NT format; for example:

NTLM: \\domainname\username. If you are using LDAP-based directories on the Websense Enterprise server, the *User Name* is in the format:

LDAP://o-domain/ou-sales/username.

If you are unsure about entering a User Name, leave the field blank and consult your Websense documentation for more information.

If Server is unavailable for 5 secs

The default value for timeout of the server is 5 seconds but you can enter a value of between 1 and 10 seconds. If the Websense Enterprise server becomes unavailable, select one of the following:

- *Block traffic to all websites*
- *Allow traffic to all websites*

URL Cache You can configure the *URL Cache* in KB. A larger *URL Cache* can provide noticeable improvements in Internet browsing response times.

6

USING THE FIREWALL LOG AND TOOLS OPTIONS

This chapter describes the commands and options available in the *Log* menu and the *Tools* menu. Each menu is broken up into sections shown in the user interface as tabs.

To access a command click on either *Log* or *Tools* and then on the appropriate tab.

The following sections are covered in this chapter:

- [Logs and Alerts](#)
- [Viewing the Log](#)
- [Changing Log and Alert Settings](#)
- [Generating Reports](#)
- [Restarting the Firewall](#)
- [Managing the Firewall Configuration File](#)
- [Upgrading the Firewall Firmware](#)

Logs and Alerts

The Firewall maintains an event log, which contains events that may be security concerns. You can view this log using the Firewall Web interface or you can set up a tab-delimited text file to be sent automatically and periodically to any e-mail address for convenience and archival purposes.

If you want to be alerted of high-priority information, such as an attack on a server, you can specify that this information is immediately e-mailed, either to the main e-mail address used by the log, or to a different address, such as a paging service.

The Firewall logs the following events:

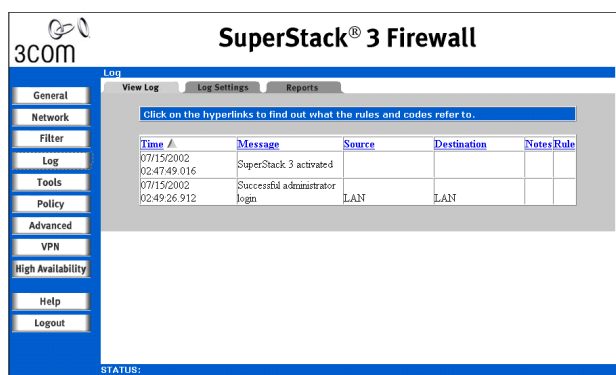
- Unauthorized connection attempts

- Blocked Web, FTP and Gopher sites, and blocked NNTP Newsgroups
- Blocked ActiveX and Java
- Blocked Cookies and Proxy attempts
- Attacks such as IP spoofing, Ping of Death, SYN flood
- Administrator logins
- Successful/unsuccessful loading of the Web Site Filter

Viewing the Log

To view the log click *Log* and then select the *View Log* tab. A window similar to that in [Figure 36](#) displays.

Figure 36 View Log Window



The log is usually displayed as a list in a table, but may appear differently depending on the browser used. You may have to adjust the browser's font size and other viewing characteristics to display the log data most efficiently. Depending on the browser, you can copy entries from the log and paste them into documents. Alternatively, use the *E-mail Log* function and review the log with an e-mail client rather than with a Web browser.

Each log entry contains the date and time of the event, and a brief message describing the event. Some entries contain additional

information. Much of this information refers to the Internet traffic passing through the Firewall.

TCP, UDP, or ICMP packets dropped

These log messages describe all traffic blocked from the Internet to the LAN. The source and destination IP addresses of the packet is shown. If the packet was TCP or UDP, the port number, in parentheses, follows each address. If the packet was ICMP, the number in parentheses is the ICMP code. The address information is usually preceded by the name of the service described by either the TCP or UDP port, or the ICMP type in quotation marks.

Web, FTP, Gopher, or Newsgroup blocked

The LAN IP and Ethernet addresses of a machine that attempted to connect to the blocked site or newsgroup is displayed. In most cases, the name of the site which was blocked is also shown. In addition, there is a box labeled *Rule* which contains one or more lowercase letters. These correspond to the categories in the Web Site Filter as follows:

- a = Violence/profanity
- b = Partial nudity
- c = Full nudity
- d = Sexual acts
- e = Gross depictions
- f = Intolerance
- g = Satanic/cult
- h = Drug culture
- i = Militant/extremist
- j = Sex education
- k = Gambling/illegal
- l = Alcohol/tobacco

See [Chapter 11](#) for more information about these categories.

ActiveX, Java, or Code Archive blocked

The IP addresses of the source machine and the destination server is shown.



When ActiveX or Java code is compressed into an archive it is not always possible to differentiate between the two. If either ActiveX or Java blocking is enabled, all code archives are blocked.

Cookie blocked

The IP addresses of the local machine and the remote server are shown.

Ping of Death, IP Spoof, and SYN Flood Attacks

The IP address of the destination machine which may be under attack, as well as the source address which appears in the packet are shown. In these attacks, the source address shown is usually fake and usually cannot be used to determine the source of the attack.

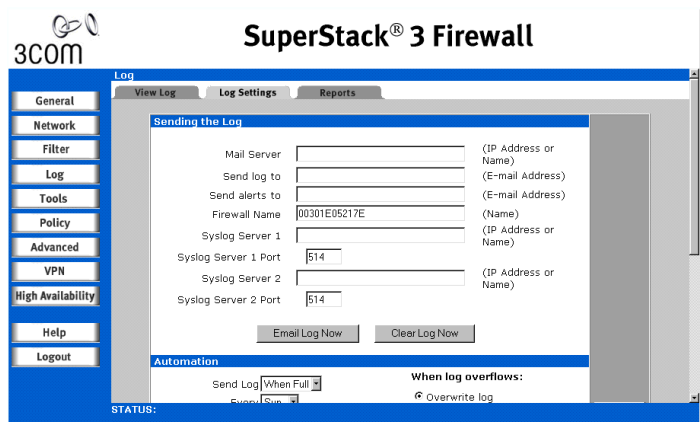


Varying conditions on the Internet can produce conditions which may cause the appearance of an attack, even when no-one is deliberately attacking one of the machines on the LAN or DMZ. This is particularly true for SYN Flood attacks. If the log message calls the attack “possible”, or it only happens on an irregular basis, then there is probably no attack in progress. If the log message calls the attack “probable”, contact the ISP to see if they can track down the source of the attack. In either case, the LAN and DMZ are protected and you do not need to take further steps.

Changing Log and Alert Settings

Click *Log* and then select the *Log Settings* tab. A window similar to that in [Figure 37](#) displays.

Figure 37 Log Settings Window



Sending the Log

Use the Sending the Log feature to inform your administrator of the performance of the Firewall and to make sure that the log file always has space for new entries.

Mail Server

To enable sending log or alert messages via e-mail, you must specify the numerical IP address or the name of your SMTP server or use a local SMTP server if available. You can obtain this information from the Internet Service Provider that you use to connect the network to the Internet. If you leave this box blank, log and alert messages are not sent via e-mail.

Send Log To

This is the e-mail address to which log files are sent and must be a fully qualified address, for example, `username@3Com.com`. Once sent, the log file is cleared from the Firewall's memory. If you leave this box blank, log messages are not sent by e-mail. You can configure the Firewall to check on a weekly basis if new software is available for download. See ["Upgrading the Firewall Firmware"](#) on [page 109](#) for more information. If there is a new software release, an e-mail notification is sent to this address.

Send Alerts To

Alerts are events, such as an attack, which may warrant immediate attention. When an event generates an alert, a message is immediately sent to an e-mail account or e-mail pager. Enter the e-mail address, for example, `username@3Com.com`, to which alert messages are sent in this box. This may be a standard e-mail account or, quite often, a paging service. If you leave this box blank, alert messages are not sent by e-mail.

Firewall Name

A unique name for the Firewall. Enter this ID to identify the Firewall when logs and alerts are emailed to the Network Administrator. Use alphanumeric characters for this field. The MAC address of the Firewall is the default value.

Syslog Server

In addition to the standard screen log, the Firewall can write extremely detailed event log information to an external Syslog server. Syslog is an industry standard protocol used for capturing log information for devices on a network. The Firewall's Syslog captures all screen log activity, plus every connection's source and destination IP addresses, IP service, and number of bytes transferred. To support Syslog, you must have an external server running a Syslog daemon on UDP Port 514. Syslog is a standard feature of UNIX.

The Firewall supports up to two syslog servers. Enter the Syslog server's IP address in the *Syslog Server 1* field. If you have a second or back up Syslog server, enter the IP address in the *Syslog Server 2* field.

To download the free 3Com Syslog Server visit:

<http://www.3com.com/ssfirewall>

and click the *Utility Software* link.



The Firewall supports WebTrends Firewall Suite for comprehensive reporting of the Firewall. To enable WebTrends reporting, click Log located at the left side of the browser window. Click Log Settings. On the Log Settings page, enter the IP address of the WebTrends server in the Syslog Server field. Click Update and restart the Firewall for changes to take effect.

E-mail Log Now

Click *E-mail Log Now* to send the log to the address in the *Send Log To* box and then delete the log.

Clear Log Now

Click *Clear Log Now* to delete the contents of the log.

Changing the Log Automation Settings

The Automation time set here determines when the Firewall queries the 3Com server for new firmware. To ease traffic on the network server, this time is randomized.

Send Log

This pop-up menu is used to configure the frequency of log messages being sent as e-mail: daily, weekly, or only when the log is full. If the weekly or the daily option is selected, specify a time of day when the e-mail is to be sent. If the weekly option is selected, then also specify which day of the week the e-mail is to be sent. If the weekly or daily option is selected and the log fills up, it is automatically e-mailed to the *Send Log To* address and cleared.

When log overflows

In some cases, the log buffer may fill up, which can happen if there is a problem with the mail server and the log cannot be successfully e-mailed. By default the Firewall overwrites the log and discards its contents. As a security measure, you can choose to shut down the Firewall, which

prevents any further traffic from traveling through without being logged. To do this select *Shutdown Firewall*.

Selecting the Categories to Log

Click the appropriate check box to enable the generation of the following log message categories.

System Maintenance

When enabled, log messages showing general system maintenance activity, such as administrator logins, automatic loading of Web Site Filters, activation and restarting the Firewall, are generated. This is enabled by default.

System Errors

When enabled, log messages showing problems with DNS, e-mail, and automatic Web Site Filter loading are generated. This is enabled by default.

Blocked Web Sites

When enabled, log messages showing Web sites, newsgroups, or other services blocked by the Web Site Filter, by keyword, or for any other reason are generated. This is enabled by default.

Blocked Java, ActiveX, and Cookies

When enabled, log messages showing Java, ActiveX, and Cookies which are blocked by the Firewall are generated. This is enabled by default.

User Activity

When enabled, log messages showing any successful or unsuccessful user logins are generated. This is enabled by default.

VPN TCP Stats

When enabled, log messages show VPN traffic information including data transfers through VPN tunnels.

Attacks

When enabled, log messages showing SYN Floods, Ping of Death, IP Spoofing, and attempts to manage the Firewall from the Internet are generated. This is enabled by default.

Dropped TCP

When enabled, log messages showing blocked incoming TCP connections are generated. This is enabled by default.

Dropped UDP

When enabled, log messages showing blocked incoming UDP packets are generated. This is enabled by default.

Dropped ICMP

When enabled, log messages showing blocked incoming ICMP packets are generated. This is enabled by default.

Network Debug

When enabled, log messages showing Ethernet broadcasts, ARP resolution problems, ICMP redirection problems, and NAT resolution problems are generated. This category is intended for experienced network administrators. This is disabled by default.

Denied LAN IP

When enabled, log messages showing details of any packets that were refused access to the LAN.

Alert Categories

Alerts are events, such as an attack, which may warrant immediate attention. When an event generates an alert, a message is immediately sent to the e-mail account defined in the *Send alerts to* box on the *Log Settings* window (see [page 98](#)).

Attacks

When enabled, all log entries that are categorized as an *Attack* are generated as an alert message. This is enabled by default.

System Errors

When enabled, all log entries that are categorized as a *System Error* are generated as an alert message. This is enabled by default.

Blocked Web Sites

When enabled, all log entries that are categorized as a *Blocked Web Site* are generated as an alert message. This is disabled by default.

Click *Update* to save your changes.



If you are using an SNMP Manager to monitor the Firewall, SNMP Trap messages are generated only for the selected alert messages. If none of the categories is selected, then none of the trap messages are sent out.

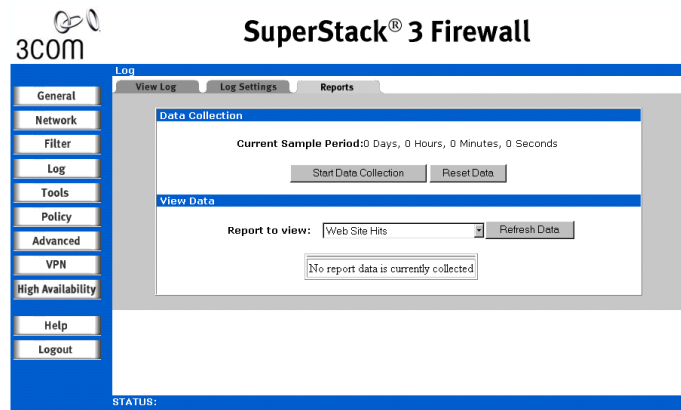
Generating Reports

The Firewall can analyze the event log to show the following:

- Top 25 most accessed Web sites
- Top 25 users of bandwidth by IP address
- Top 25 services that consume the most bandwidth

Click *Log* and then select the *Reports* tab. A window similar to that in [Figure 38](#) displays.

Figure 38 Reports Window



Collecting Report Data

Start Data Collection

By default, the log analysis function is disabled. Click *Start Data Collection* to begin log analysis. When log analysis is enabled, the button label changes to *Stop Data Collection*.

Reset Data

Click *Reset Data* to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the Firewall is restarted.

Current Sample Period

Displays the current sample period shown in the reports.

Viewing Report Data Select the desired report from the Display Report popup menu. The options are:

- *Web Site Hits*
- *Bandwidth Usage by IP Address*
- *Bandwidth Usage by Service.*

These reports are explained as follows.

Web Site Hits

Select *Web Site Hits* from the *Report to view* drop-down list to display a table showing the URL for the 25 most accessed Web sites and the number of hits to that site during the current sample period.

Use the *Web Site Hits* report to ensure that the majority of Web access is to sites considered applicable to the primary business function. If leisure, sports, or other similar sites are on this list, it may signal the need to change or more strictly enforce the organization's Acceptable Use Policy.

Bandwidth Usage by IP Address

Select *Bandwidth Usage by IP Address* from the *Report to view* drop-down list to display a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.



If using DHCP, remember that the IP address assigned to a computer can change. You may have to check the DHCP server logs to correctly identify which computer is listed in the report.

Bandwidth Usage by Service

Selecting *Bandwidth Usage by Service* from the *Report to view* drop-down list displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio and so forth, and the number of megabytes received from the service during the current sample period.

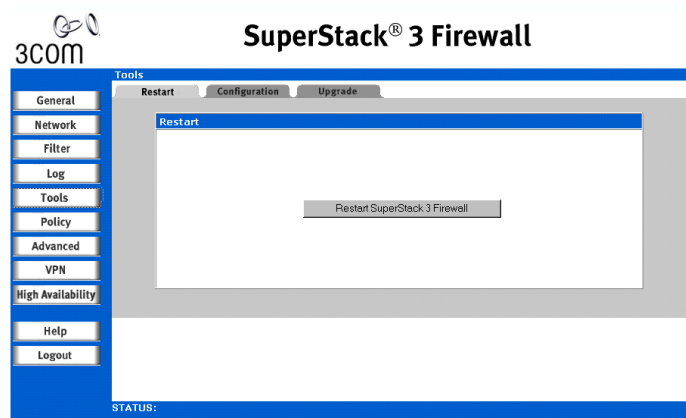
Use the *Bandwidth Usage by Service* report to make sure the Internet services being used are appropriate for the organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, it may signal the need to change or more strictly enforce the organization's Acceptable Use Policy.

Restarting the Firewall

To restart the Firewall:

- 1 Click *Tools* and select the *Restart* tab. A window similar that in [Figure 39](#) displays.

Figure 39 Restart Window



- 2 Click *Restart SuperStack 3 Firewall*.
- 3 Click *Yes* to confirm the restart and send the restart command to the Firewall. The restart takes about 90 seconds, during which time the Firewall cannot be reached from the Web browser and all network traffic through it is halted.



If you have changed the IP settings of the Firewall, you must alter the IP settings of the management station accordingly. You may have to restart the management station, depending on its operating system, for the change to take effect.

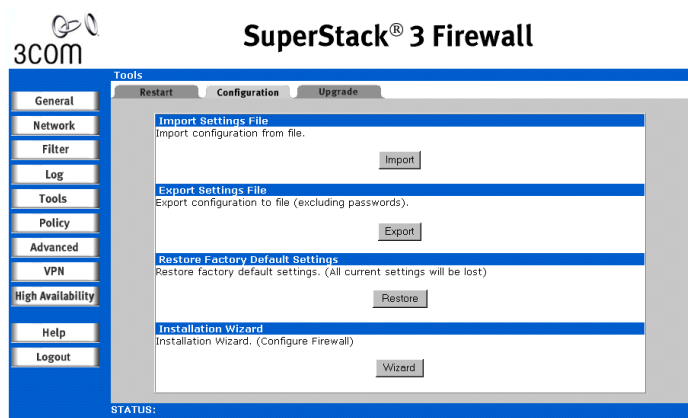
When the Front Panel Power LED stops flashing you can refresh your browser.

To reset the Firewall clearing it of all settings see [“Resetting the Firewall”](#) on [page 198](#) for details.

Managing the Firewall Configuration File

The Configuration tool allows you to save and restore the configuration settings of the Firewall. Click *Tools* and then select the *Configuration* tab. A window similar to that in [Figure 40](#) displays.

Figure 40 Configuration Window



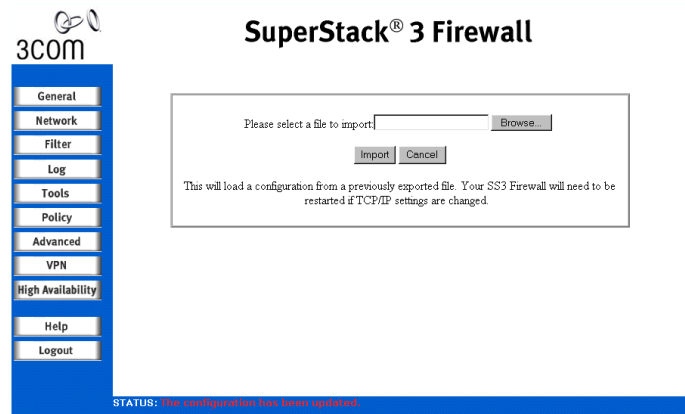
Use the *Configuration* tab to specify where the settings for the Firewall are saved to and retrieved from for backup purposes. You can also restore the default settings from the *Configuration* tab. 3Com recommends that you back up the Firewall settings.

Importing the Settings File

Use this function to import a previously saved settings file back into the Firewall.

- 1 Click *Import*. A window similar to that in [Figure 41](#) displays.

Figure 41 Import Window



- 2 Click *Browse* to find a file which was previously saved using *Export*. See [“Exporting the Settings File”](#) on [page 108](#) for more information about exporting a file.



*You may need to set File type to *.* to be able to see the.exp file you exported.*

- 3 Once you have selected the file, click *Import*.
- 4 Once the file transfer has completed the status at the bottom of the screen gives you the option to *Restart* the Firewall.
- 5 Click *Restart*.



Make sure that the Web browser supports HTTP uploads. If it does not, you cannot import the saved settings.

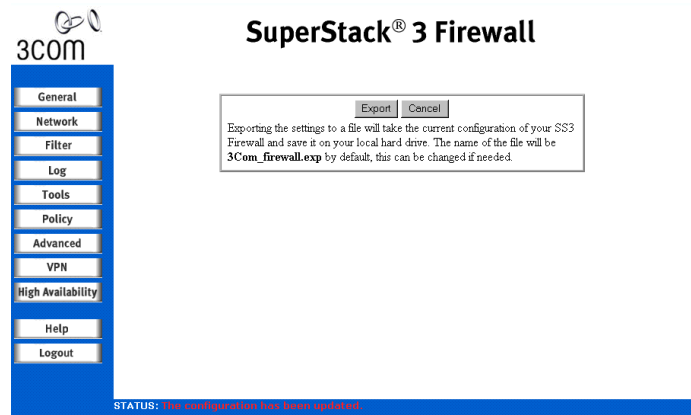
Note that this does not change the password for the unit.

Exporting the Settings File

You can save the Firewall configuration settings to a file on a local system and then reload those settings.

- 1 Click *Export*. A window similar to that in [Figure 42](#) displays.

Figure 42 Export Window



- 2 Choose the location to save the settings file. This should be saved as <Filename>.exp. This defaults to 3com_firewall.exp. The process may take up to a minute.



The Administration password is not saved to the exported file in this process.

Restoring Factory Default Settings

Click *Restore* to clear all configuration information and restore the Firewall to its factory state.



Clicking Restore does not change the Firewall's LAN IP Address, LAN Subnet Mask, WAN Gateway Address and Password.

Using the Installation Wizard to reconfigure the Firewall

Click *Wizard* to start the Installation Wizard. This allows you to configure the Firewall for a new location or role. See [Chapter 3, "Quick Setup for the Firewall"](#).

Upgrading the Firewall Firmware

The Upgrade tool allows you to upgrade the operational firmware of the Firewall. The Firewall has flash memory and can be easily upgraded with new firmware.



When upgrading the firmware, all settings are reset to factory default. 3Com recommends that you export the Firewall's configuration settings before uploading new firmware and then import them again after the upgrade has been completed.

The Firewall checks to see if new firmware is available for download on a weekly basis. If there is a new firmware release, you can configure the Firewall to send an e-mail notification to the address in the *Send log to* box.

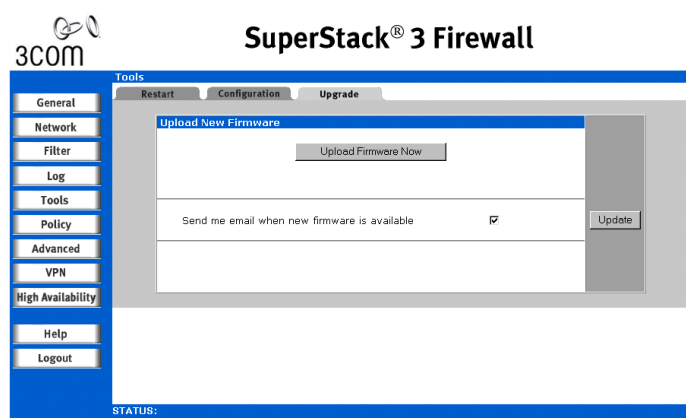
Click *Tools* and then select the *Upgrade* tab. A window similar to that in [Figure 43](#) displays.

To be notified automatically when new firmware is available:

- 1 Click the *Send me e-mail when new firmware is available* check box.
- 2 Click *Update*.

To see how to obtain new firmware go to <http://www.3com.com/ssfirewall> and follow the instructions.

Figure 43 Upgrade Window



To upload the new firmware onto the Firewall:

- 1 Click *Upload Firmware Now*.

A window similar to that in [Figure 44](#) displays.

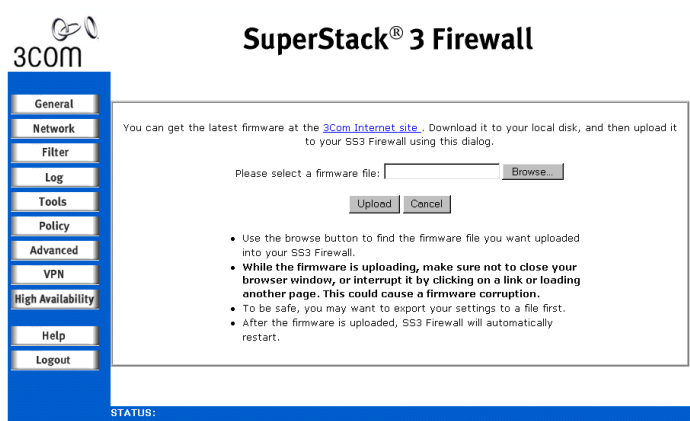
Figure 44 Save Settings Window



- 2 Click Yes if you have saved the settings.

A window similar to that in [Figure 45](#) displays.

Figure 45 Firmware Upload Window



- 3 Click *Browse...* and select the firmware file you have downloaded from the 3Com FTP site to a local hard drive or server on the LAN.
- 4 Click *Upload* to begin the upload.



When uploading the firmware to an Firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, loading a new page, or removing the power to the Firewall. If the Firewall is interrupted this way, it may result in the Firewall not responding to attempts to log in. If your Firewall does not respond, see [Chapter 12, "Troubleshooting"](#).



Make sure that your Web browser supports HTTP uploads.

Restart the Firewall for the changes to take effect.

7

SETTING A POLICY

This chapter describes the commands and options available in the *Policy* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click *Policy* and then on the appropriate tab.

The following sections are covered in this chapter:

- [Changing Policy Services](#)
- [Adding and Deleting Services](#)
- [Adding and Editing Policy Rules](#)
- [Configuring Users](#)
- [Configuring the Firewall to use a RADIUS Server](#)
- [Configuring Management](#)

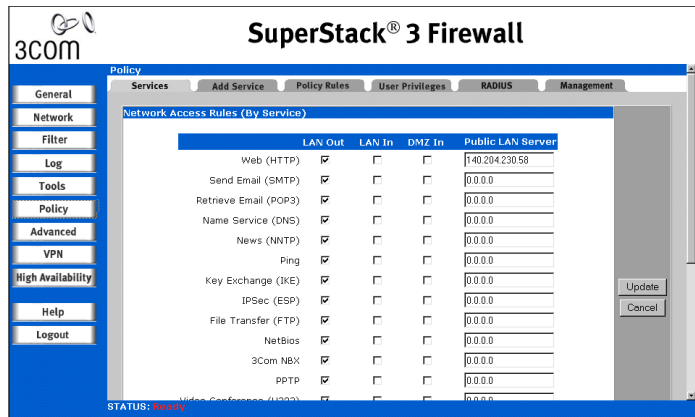
See [Chapter 11](#) for background information about policies.

Changing Policy Services

This section covers which network services are blocked by the Firewall and which are allowed to pass through.

Click *Policy*, and then select the *Services* tab. A window similar to that in [Figure 46](#) displays.

Figure 46 Services Window



Amending Network Policy Rules

The *Services* window contains a table showing the defined *Network Policy Rules*. At the bottom of the table is the *Default* rule which affects all IP services. Any rules you create for a specific protocol override the *Default* rule with respect to that protocol.

LAN Out

Click the *LAN Out* check box for a specific protocol, to allow users on the LAN access to servers of that type on the Internet. When the check box is cleared, users on the LAN *cannot* access servers of that type on the Internet. The default value is enabled. When the *Warning* icon is displayed to the right of the check box, there is a Custom Rule in the *Rules* tab section that modifies the behavior of the listed Network Access Rule.

LAN In

Clear the *LAN In* check box to prevent access to the protocol from the WAN to the LAN and, if appropriate, from the DMZ to the LAN. When the box is checked, users on the WAN and DMZ can access all hosts on the LAN via that protocol. The default value is disabled; use caution when enabling. When the *Warning* icon is displayed to the right of the check box, there is a Custom Rule in the *Rules* tab section that modifies the behavior of the listed Network Access Rule.



The LAN In column is not displayed if NAT is enabled.

DMZ In

If you are using the DMZ port on the Firewall access to the protocol is not permitted from the Internet to the DMZ when this check box is cleared. When the box is checked, users on the Internet can access all hosts on the DMZ via that protocol. The default value is enabled. When the *Warning* icon is displayed to the right of the check box, there is a Custom Rule in the *Rules* tab section that modifies the behavior of the listed Network Access Rule.

Public LAN Server Address

A Public LAN Server is a single host on the LAN that is defined to handle all traffic originating from the Internet to the LAN of a specific protocol, such as HTTP. Define a Public LAN Server by typing its IP address in the *Public LAN Server* box for that protocol. If a server is not designated for a certain protocol, type 0.0.0.0 in the box.

Changing NetBIOS Broadcast Settings

Systems running Microsoft Windows Networking communicate with one another through NetBIOS broadcast packets. By default, the Firewall blocks these broadcasts. If you have Windows computers on more than one port of the Firewall, for example if you are using the Firewall as an internal security measure you may need to enable *NetBios Broadcast Passthrough*.

From LAN to DMZ

Check this box to allow Windows machines connected to the LAN port to see other Windows machines connected to the DMZ port in their Network Neighborhood.

Click *Update* to save your changes.

From LAN to WAN

Check this box to allow Windows machines connected to the LAN port to see other Windows machines connected to the WAN port in their Network Neighborhood.

Click *Update* to save your changes.



NetBIOS passthrough only applies to connections made by using Windows Networking. You can still see web servers using the HTTP protocol even if both NetBIOS Passthrough boxes are left unchecked.

Enabling Detection Prevention

Enable Detection Prevention

By default, the Firewall responds to incoming connection requests as either *blocked* or *open*. If you check the box to enable *Detection Prevention* and click *Update*, no response is made to inbound requests, which makes your network invisible to potential attackers.

Randomize IP ID

Use this check box to prevent hackers using various tools to detect the presence of the Firewall. IP packets are given random IP IDs which makes it more difficult for hackers to *fingerprint* the Firewall. Use this check box for additional security from hackers.

Setting the Network Connection Inactivity Timeout

If a connection to a server outside the LAN remains idle for more than 5 minutes (default value), the Firewall closes the connection. This is done for security purposes. Without this timeout, it is possible that connections could stay open indefinitely, creating potential security risks. You can increase the timeout interval if users frequently complain of dropped connections in applications such as Telnet and FTP.

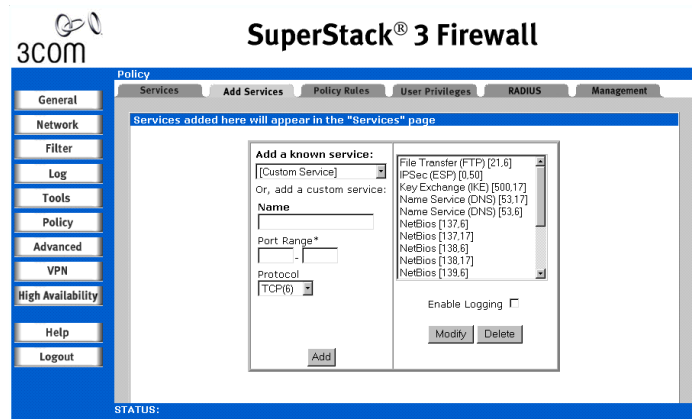
Click *Update* to save your changes.



You must restart the Firewall for these changes to take effect.

Adding and Deleting Services

If a protocol is not listed in the *Services* window, you can add the service. Click *Policy*, and then select the *Add Service* tab. A window similar to that in [Figure 47](#) displays.

Figure 47 Add Service Window

The scroll list on the right side of the screen displays all IP protocols that are currently defined and that appear in the *Services* window. Next to the name of the protocol, two numbers appear in brackets. The first number indicates the IP port number which defines the service (either *TCP Port*, *UDP Port*, or *ICMP Type*). The second number indicates the IP protocol type (6 for TCP, 17 for UDP, or 1 for ICMP).



There may be more than one entry with the same name. For example, the default configuration has two entries labeled Name Service (DNS). These are UDP port 53 and TCP port 53. Any entries with identical names are grouped together, and are treated as a single service. Up to 64 entries are supported.

Adding Support for a Known Service

To add a service known to the Firewall:

- 1 Select the name of the service from the *Add a known service* drop-down list.
- 2 Click *Add*.

The new service appears in the list box to the right, along with its numeric protocol description. Note that some well-known services add more than one entry to the list box.

Adding a Custom Service

To add a custom service:

- 1 From *Add a known service* drop-down list, select *Custom Service*.
- 2 In the *Name* box, type a unique name, such as **CC:mail** or **Microsoft SQL**.
- 3 In the *Port* box, type the IP port number or range of ports.
- 4 From the *Protocol* drop-down list, select the IP protocol type.
- 5 Click *Add*.

The new service appears in the list box.

For a list of IP port numbers, see:

<http://www.ietf.org/rfc/rfc1700.txt>



If you create multiple entries with the same name, they are grouped together as a single service and may not function as expected.

Disabling Screen Logs

You can disable the log of events which is usually written to the Firewall's internal Screen Log. For example, if LINUX's authentication protocol is filling the log with entries, you can configure the screen log to ignore all activity for this service. To disable screen logs for a specific service:

- 1 Highlight the service name in the list box.
- 2 Clear the *Enable Logging* check box
- 3 Click *Modify*.

Deleting a Service

To delete a service:

- 1 Highlight its name in the list box.
- 2 Click *Delete*.

For services with multiple entries, you can delete only a single Port/Protocol combination from the list. For example, deleting the entry marked *Name Service (DNS) [53,6]* deletes just the TCP portion of the service.

Adding and Editing Policy Rules

Network Access Policy Rules evaluate network traffic's source IP address, destination IP address, and IP protocol type to decide if the IP traffic is allowed to pass through the Firewall. Custom rules take precedence, and may override the Firewall's default state packet inspection. Up to 100 policy rules may be entered.



CAUTION: The ability to define Network Access Rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting Network Access Rules.

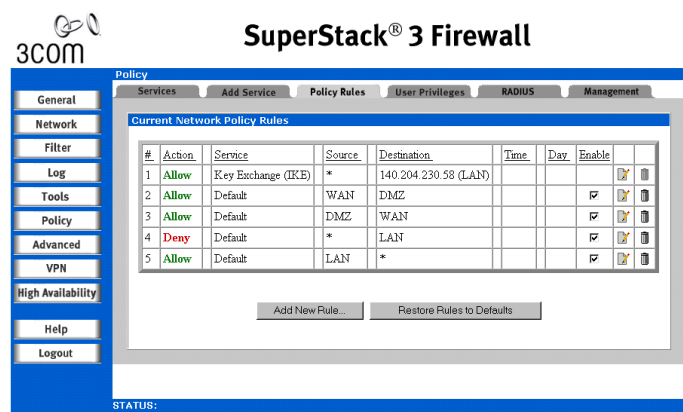


Network Access Rules do not disable protection from Denial of Service attacks, such as SYN Flood, Ping of Death or LAND. However, it is possible to create vulnerabilities to attacks that exploit vulnerabilities in applications, such as WinNuke.

Viewing Network Policy Rules

Click *Policy*, and then select the *Policy Rules* tab. A window similar to that in [Figure 48](#) displays.

Figure 48 Policy Rules Window



The *Current Network Policy Rules* table is an extension of the *Services* display covered in [“Changing Policy Services”](#) on [page 113](#). In this display you can see the default rules and any rules you have created. You can use this screen to fine-tune services and add exceptions.

Rules are arranged in order of precedence from the most specific to the most general.

For example if you block all FTP traffic in one rule and allow a machine with a specific IP address to use FTP in another rule then the second rule overrides the first and is displayed above it.

The table is divided into columns as follows:

Rule Number (#)

Rules are consecutively numbered by precedence and new rules are inserted into the list by the Firewall at a position appropriate to the breadth of scope of the rule.

When evaluating rules, the Firewall uses the following criteria:

- 1 A rule defining a specific service is more specific than the default rule.
- 2 A defined Ethernet link, such as LAN, WAN, or DMZ, is more specific than * (all).
- 3 A single IP address is more specific than an IP address range.

Action

The *Action* for a rule can be set to either *Allow* or *Deny* traffic across the Firewall. For security reasons common protocols are often denied and more specific rules created to describe where these protocols are used legitimately.

Service

The *Service* for a rule shows the service (and hence the protocol) over which the rule operates. A value of *Default* indicates that the rule operates on all traffic. Other values for *Service* are defined in [“Adding and Deleting Services”](#) on [page 116](#).

Source

The *Source* of a rule indicates where the connection for that rule is originated. The source can be set to LAN, DMZ, WAN or an specific address or range of addresses on one of those ports.



When a connection is made a two-way conversation is initiated. When allowing a PC on the LAN network port to communicate with a PC or Server on the WAN network port (e.g. to Browse using HTTP) it is unnecessary (and inadvisable) to set a rule for the reverse journey. This would only be necessary if you wanted the server on the WAN to initiate connections with the PC on the LAN network port.

Destination

The *Destination* for a rule refers to the target of the connection made by the source. As with the *Source* this can be set to a network port specific address or range of addresses.

Time

The *Time* of a Rule shows the hours between which it operates.

Day

The *Day* of a rule shows the days on which it operates.

Enable

The *Enable* check box shows whether a rule is currently active. To activate a rule check the box. To deactivate a rule clear the check box.

Edit (no column heading)

To Edit the settings for a rule click on the icon of a pencil and paper for the rule you want to edit. Clicking on the icon opens the *Edit Rule* window where you can make the changes you need. In the *Edit Rule* window:

- To save your changes click *Update*.
- To leave the Edit Rule window without saving changes close it using the Windows close option.
- To reset all the parameters of the rule to the values they were before you started editing click *Reset*. This saves no changes and allows you to continue editing.

Delete (no column heading)

To *Delete* the settings for a rule click on the icon of the trash can for the rule you want to edit. Clicking on the icon opens a dialog box asking you to confirm the action. Click *OK* to delete the rule. Click *Cancel* if you clicked on the trash can in error.



If you want to stop using a rule which you may want to use again, consider clearing the Enable check box rather than deleting the rule.

Adding a New Rule

When you click *Add New Rule*, the screen shown in [Figure 49](#) is displayed.

Figure 49 Add New Rule Window

Add Rule - Microsoft Internet Explorer

Add Network Access Rule

Action ☒ Allow ☐ Deny

Service

Ethernet Addr Range Begin Addr Range End

Source

Destination

Apply this rule to to (24-Hour Format)

Inactivity Timeout in Minutes

Allow Fragmented Packets ☐

Settings below will not take effect until enabled on Advanced Ethernet page.

☐ Enable Outbound Bandwidth Management

Guaranteed Bandwidth kbps

Maximum Bandwidth kbps

Bandwidth Priority

Fill in the fields that you want to change. To keep the field general rather than use a specific value leave the field at its default value.

All fields can be left as default apart from the *Action* field which must have either *Allow* or *Deny* selected.

Allow Fragmented Packets

By default the Firewall drops fragmented packets as they may form part of a Denial of Service attack. Fragmented packets can occur naturally and you may want to allow them to allow certain traffic through your Firewall.

Fragmented packets that are dropped show as entries in the Firewall Log. See [“Viewing the Log”](#) on [page 96](#) for details.

Bandwidth Management

The Firewall can be configured for bandwidth management of outbound (WAN) network traffic using the bandwidth management options. Each Service that you add using a Policy Rule has a check box to enable Bandwidth Management for the Service. Select *Enable Bandwidth Management* and then enter the guaranteed bandwidth in Kbps for the Service. Before you can enable and configure bandwidth management for Policy Rules, you must enable it on the *Ethernet* tab that you can select from the *Advanced* menu. See [“Configuring the Ethernet Port Settings”](#) on [page 147](#) for more information.



CAUTION: *Bandwidth management is very complex and requires extensive knowledge of networks and networking protocols. Incorrect bandwidth management can cause network problems or degradation of network performance. See [“Bandwidth Management”](#) on [page 228](#) for an overview of this function.*

Restoring Rules to Defaults

To remove all the custom rules click *Restore Rules to Defaults*. This removes all the custom rule that have been added and restores the four rules that are implemented as default.

Configuring Users

User level access can be configured for authentication and access to the network. Authentication can be performed using the Firewall's local user database, Radius or a combination of the two applications. This gives authorized users access to the LAN from remote locations on the Internet as well as a means to bypass the Internet filtering and blocking from the LAN to the Internet. These users are known as *Privileged Users*.

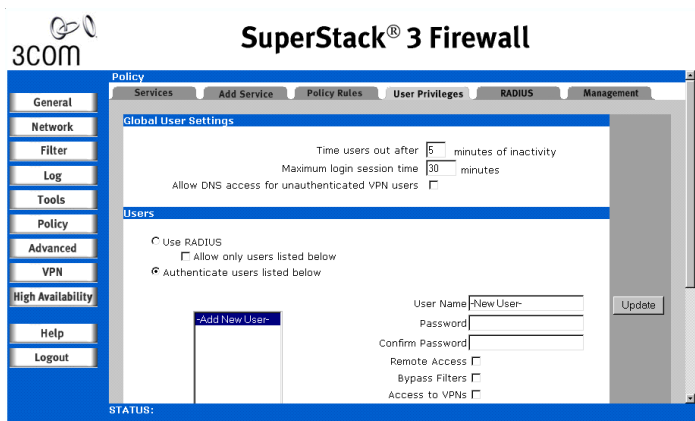


Privileged Users can only use the Services currently allowed by the Firewall. If an external user needs full access to your LAN you need to create a Virtual Private Network (VPN) connection to allow the traffic. See [“Configuring Virtual Private Network Services”](#) on [page 151](#) for instructions on configuring VPN on the Firewall and [“Networking Concepts”](#) on [page 215](#) for VPN background information.

By default when a VPN tunnel is established between two Firewalls, any users on the LAN port of each Firewall can send data across the VPN. In some cases complete user access could be a security risk and you may want to allow only authenticated users to access the VPN tunnel and send data across the network.

Click *Policy*, and then select the *User Privileges* tab. A window similar to that in [Figure 50](#) displays.

Figure 50 Users Window



Global User Settings Timeout

Enter the number of minutes a user can be inactive before being automatically logged out of the network by the Firewall.

Max Login Session Time

Enter the time in minutes that a user is allowed to be logged into the network through the Firewall. When a user logs into the Firewall using his username and password, the user can also set the maximum login session time but it cannot be longer than the time configured by the system administrator. For unlimited login session time, set this value to 0 (zero).

Allow DNS for unauthenticated VPN Users

If you check this box, unauthenticated users can access a DNS server over the VPN tunnel that normally has authentication enforced.

Setting User Privileges

Use RADIUS

Select this option if you have configured RADIUS to authenticate users accessing the network through the Firewall. If you have more than 100 users who require authentication, you must use RADIUS. If you select *Use RADIUS*, users must log into the Firewall using HTTPS in order to encrypt the password sent to the Firewall. If a user attempts to login using HTTP, the browser is automatically redirected to HTTPS.

See [“Configuring the Firewall to use a RADIUS Server”](#) on [page 127](#) for information about authenticating user privileges with a RADIUS server.

Allow only users listed below

Check this box if you have a subset of RADIUS users accessing the Firewall. The user names must be added to the Firewall's internal database before they can be authenticated using RADIUS.

Authenticate users listed below

If you select this option, you can add users to the Firewall's internal database for authentication.

User Name

This is the user's login name.

Password and Confirm Password

Enter the password in the *Password* and *Confirm Password* field. The password is case-sensitive.

Remote Access

Check this box if the user accesses LAN resources through the firewall from a remote location on the internet.



If you enable Remote Access, you allow unencrypted traffic over the internet. 3Com recommends that you use VPNs instead for security reasons.

Bypass Filters

Check this box if the user has unlimited access to the Internet from the LAN port and can bypass Web, News Java and ActiveX blocking.

Access to VPNs

Check this box if the local LAN user can send information over the VPN Security Associations with authentication enforcement.

Access to L2TP VPN Client

Check this box if the remote user accesses the firewall through an L2TP VPN client.

Access from VPN Client with XAUTH

Check this box if the remote user requires XAUTH for authentication and accesses the firewall through a VPN client.

Limited Management Capabilities

Check this box to provide the user with limited management of the Firewall over the Web interface. Access is limited to:

- **General** — *Unit Status, Set Time*
- **Log** — *View Log, Log Settings, Log Reports*
- **Tools** — *Restart, Network Diagnostics (less Tech Support Report)*

Adding Users

To add a new user:

- 1 Highlight the *Add New User* entry.
- 2 In the *User Name* box, type the user's login name.
- 3 In the *Password* and *Confirm Password* boxes, enter the user's password.

It is important to use a password that could not be guessed by someone else. Avoid using names of friends, family, pets, places, and so on. Good passwords can be created by:

- Making up nonsense words, such as `dwizdell`
- Including non-alphanumeric ASCII characters in words, such as `thr3c#m`

Passwords are case sensitive.

- 4 Choose the privileges to be enabled for the user by checking boxes. See the previous section for a description of these functions.
- 5 Click *Update* to save your changes.



The maximum number of Privileged Users the Firewall allows is 100.



User names are not case sensitive; typing `joe` is equivalent to typing `JOE` or `Joe`. Passwords are case sensitive; typing `password` is not the same as typing `Password`).

Changing Passwords and Privileges

To change a user's password or privileges:

- 1 Highlight the name in the scrollable box.
- 2 Make the changes.
- 3 Click *Update User*.

Deleting a User

To delete a user, highlight the name and click *Remove User*.



To configure a user's machine to support privileged users see ["Establishing an Authenticated Session"](#) below.

Establishing an Authenticated Session

Authenticated Sessions allow a user on the Internet to access the LAN without restrictions, or allow a user on the LAN to access the Internet without restrictions, bypassing the Web Site Filters.



Make sure that the Web browser software being used to establish an authenticated session supports Java, JavaScript or ActiveX scripting.

To establish an Authenticated Session, enter your Firewall's LAN IP Address at the Web browser. This process is identical to the administrator login.

A dialog box is displayed, asking you for the user name and password. After filling in these boxes and clicking *Login*, the password is verified using MD5 authentication. The password is never sent *in the clear* over the Internet, preventing password theft and replay attacks.

Once authenticated, remote users can access all IP resources on the LAN, and users on the LAN can bypass the Web Site Filter. The connection closes if user inactivity on the connection exceeds the configured time-out period. In that case, the remote user must re-authenticate. If it seems like authentication is failing for no reason, make sure that the Caps Lock key on your keyboard is not on.



You cannot use remote authenticated access when NAT is enabled.

Configuring the Firewall to use a RADIUS Server

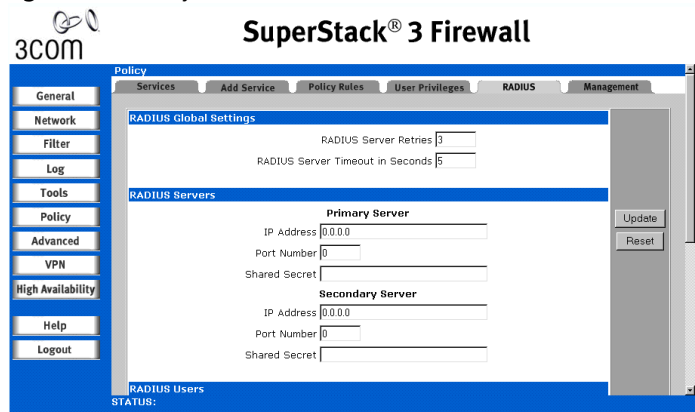
The Firewall is capable of using a RADIUS (Remote Authentication Dial-In User Service) server to authenticate users. Before using RADIUS to authenticate VPN clients enable *Require authentication of VPN clients via XAuth* in the *Advanced Settings* of a Security Association. See ["Security Policy Settings for IKE using Pre-Shared Secret"](#) on [page 155](#).



CAUTION: *The RADIUS server can only authenticate client devices. Do not enable Xauth authentication if you are authenticating with another Firewall.*

Click *Policy* then click *RADIUS*. A window similar to the one in [Figure 51](#) is displayed.

Figure 51 Policy Radius Window



**Configuring the
Radius Global
Settings**

RADIUS Server Retries

Enter the number of times you want the Firewall to attempt to connect to the RADIUS Server in the *RADIUS Server Retries* field. If the RADIUS server does not respond within the specified number of retries, the user authentication fails. This field may range between 0 and 30. A value of 3 is recommended for a typical network.

RADIUS Server Timeout in Seconds

The *RADIUS Server Timeout in Seconds* field determines the length of time that will elapse before the Firewall attempts to contact the RADIUS server again after a failure. The RADIUS server timeout may range from 0 to 60 seconds. A value of 5 seconds is recommended for a typical network.

**Specifying the
RADIUS Servers**

The primary RADIUS server is defined in the RADIUS server section. An optional secondary RADIUS server may be defined if a backup RADIUS server exists on the network.

The process for configuring a primary RADIUS server is described below. If you have a backup or secondary RADIUS server on your network then repeat the process for the *Secondary Server* fields.

Name or IP Address

Enter the DNS name or IP address of your RADIUS server in the *Name or IP Address* field. Using the name of the server allows you to change its address without reconfiguring the Firewall.

Click *Update* to save your changes.

Port Number

Enter the UDP port number that your RADIUS server listens on in the *Port Number* field. This information can be found in the documentation that came with your RADIUS server.

The *Steel-Belted RADIUS Server*, for example, is set to listen on port 1645 by default.

Click *Update* to save your changes.

Shared Secret

The shared secret of a RADIUS server is a case sensitive alphanumeric string of up to 30 characters that is used to authenticate the Firewall and the RADIUS server. Your RADIUS server may use its administrative password as a shared secret.

Enter the shared secret or administrative password of your RADIUS server in the Shared Secret Field.

Click *Update* to save your changes.



When configured for a RADIUS server the Firewall records both successful and failed User Logins using XAUTH/RADIUS.

**Configuring RADIUS
User Privileges**

If you want all RADIUS users to be able to access the Firewall you need only set the default privileges for all RADIUS users on this tab. If you want a sub-section of RADIUS users to be able to access the Firewall you must also configure the RADIUS server to do this. See [“RADIUS Server Configuration”](#) on [page 231](#) for more information.

Remote Access

Enable this check box if the user accesses the Firewall from a remote computer. This option is only available in *Standard* mode.

Bypass Filters

Enable *Bypass Filters* if the LAN user can bypass Content Filter settings.

Access to VPNs

Enable the check box if the user can send information over VPN security associations.

Access from L2TP Client

Enable this check box if you have remote users accessing the Firewall using L2TP VPN clients and authenticating through RADIUS and the Firewall's L2TP server.

Access from VPN Client with XAUTH

Enable the check box if a remote user accesses the Firewall with a VPN client using XAUTH for authentication.

Limited Management Capabilities

By enabling this check box, the user has limited local management access to the Firewall management interface. The access is limited to the following functions:

- **General** — *Unit Status, Set Time*
- **Log** — *View Log, Log Settings, Log Reports*
- **Tools** — *Restart, Network Diagnostics (less Tech Support Report)*

Configuring the RADIUS Client Test

You can test your RADIUS Client user name and password by entering a valid *User name* and the *Password* and then clicking *Update*. If the validation is successful, the *Status* messages changes to *success*. If the validation fails, the *Status* message changes to *failure*.

Once the Firewall has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to enter a *User Name* and *Password* into a dialogue box.

Configuring Management

Click *Policy* and then click the *Management* tab. A window similar to the one shown in [Figure 52](#) displays. This screen allows you to configure how the Firewall is managed. It can be monitored remotely using an SNMP (Simple Network Management Protocol) management system such as

3Com Network Supervisor or managed locally and/or remotely using the Web interface.

3Com strongly recommends that you use https management as this is more secure. See [“HTTPS Management”](#) on [page 134](#) for more information.

Figure 52 Policy Management Window

The screenshot shows the 'SuperStack® 3 Firewall' web interface. The left sidebar contains a menu with options: General, Network, Filter, Log, Tools, Policy, Advanced, VPN, High Availability, Help, and Logout. The main window has tabs for Policy, Services, Add Service, Policy Rules, User Privileges, RADIUS, and Management. The 'Policy' tab is active, and the 'SNMP' sub-tab is selected. The SNMP configuration form includes a checkbox for 'Enable SNMP', which is checked. Below this are input fields for 'System Name:', 'System Contact:', and 'System Location:'. Further down are 'Get Community Name:' (with 'public' entered) and 'Trap Community Name:'. At the bottom of the form are four 'Host' input fields labeled 'Host 1:', 'Host 2:', 'Host 3:', and 'Host 4:'. On the right side of the form are 'Update' and 'Cancel' buttons. The status bar at the bottom indicates 'Management Method' and 'STATUS:'.

Configuring SNMP Management

SNMP (Simple Network Management Protocol), is a network protocol that provides network administrators with the ability to monitor the status of the Firewall and receive notification of any critical events as they occur on the network. The Firewall supports SNMP v1/v2c and all relevant Management Information Base II (MIB-II) groups except egp and at. The Firewall replies to SNMP Get commands for MIB-II via any interface and supports a custom MIB for generating trap messages.

The following standard MIB-II (RFC 1213) MIBs are supported:

- system
- interfaces
- ip
- icmp
- tcp
- udp
- snmp

To configure SNMP, enter the necessary information in the following fields:

Enable SNMP

SNMP is disabled by default. To enable the SNMP agent, select *Enable SNMP*.

System Name

This is the hostname of the Firewall.

System Contact

Type in the name of the network administrator for the Firewall.

System Location

The network administrator's contact information can be entered in this field. Enter an e-mail address, telephone number, or pager number.

Get Community Name

Create a name for a group or community of administrators who can view SNMP data. The default value is *Public*.

Trap Community Name

Create a name for a group or community of administrators who can receive SNMP traps. A name must be entered.

Host 1 through 4

Enter the IP address or hostname of the SNMP management system receiving the SNMP traps. Up to 4 addresses or hostnames can be specified.

Configuration of the Log/Log Settings for SNMP

Trap messages are generated only for the categories that alert messages are normally sent, i.e. attacks, system errors, blocked web sites. If none of the categories is selected on the *Log Settings* page, then none of the trap messages are sent out.

Configuration of the Service and Rules Pages

By default, the Firewall responds only to SNMP Get messages received on its LAN interface. Appropriate rules must be set up in the Firewall to allow SNMP traffic into the trusted network. SNMP trap messages may be sent

via the LAN, WAN, or DMZ interface. If your SNMP management system supports discovery, the SNMP agent should automatically discover the appliance on the network. Otherwise, you need to add the appliance to the list of SNMP manageable devices on the SNMP management system.

Setting the Management Method

You can manage your Firewall locally, or remotely from a remote host such as a laptop.

The first step in setting up the management of the Firewall, is selecting the managing method to be used.

- *From the LAN interface* is the default and allows you to manage the Firewall from a web browser on the LAN network. When operating in this mode, no Security Association information is needed.
- *From the LAN interface and remotely, from the WAN interface* allows you to manage your Firewall from a remote host. When operating in this mode, you must specify Security Association information so that network traffic between your the Firewall and the remote host is secure. You must also install a VPN Client on the remote host and configure it as described in the following section:

Manage Using Internet Explorer

If you manage the Firewall using Internet Explorer check the *Manage Using Internet Explorer* box. This allows the Firewall to use Internet Explorer specific code and speeds up management.

Click *Update* to save your changes.

Selecting Remote Management

When remote management is selected, a Management SA is automatically generated. The Management SA uses Manual Keying to set up a VPN tunnel between the Firewall and the VPN client. The Management SA also defines Inbound and Outbound Security Parameter Indices (SPIs) which match the last eight digits of the Firewall's serial number. The preset SPIs are displayed in the Security Association Information section.

- 1 Enter a 16 character hexadecimal encryption key in the Encryption Key field or use the randomly generated key that appears in the Encryption Key field. Valid hexadecimal characters are 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E and F. An example of a valid encryption key is:

1234567890ABCDEF

- 2 Enter a 32 character hexadecimal authentication key in the Authentication Key field or use the randomly generated key that appears in the Authentication Key field. An example of a valid authentication key is:

1234567890ABCDEF1234567890ABCDEF.

- 3 Click *Update* and then restart the Firewall for the change to take effect.

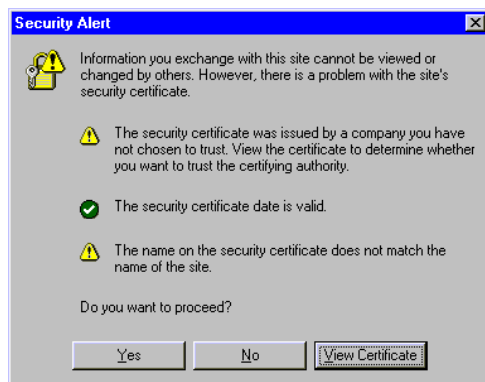
HTTPS Management

To enhance the security of the Firewall, HTTPS Management using Secure Socket Layer (SSL) is supported when you log into the Web interface using `https://IPAddress` where the *IPAddress* is the Firewall LAN IP address.

For example, if the LAN IP address of your Firewall is 192.168.168.1, you can log into it by typing `https://192.168.168.1`. Access is encrypted using SSL technology for a secure connection. HTTPS Management allows secure access to the Firewall without a VPN client. It is a simple and secure way to manage your Firewall from both the LAN and the WAN.

The first time you access the Firewall's Web interface using HTTPS, a warning dialog box similar to the one shown in [Figure 53](#) opens with a message about certificate compliance asking you to confirm you want to use HTTPS. Click Yes to continue the log in process. SSL is supported by Netscape 4.7 and higher, as well as Internet Explorer 5.5 and higher.

Figure 53 Security Alert Warning Dialog



HTTPS Management Port

You can configure the port used for HTTPS authentication. If you use a port other than the default of 443, you may add another layer of security to the management of the firewall. Enter the preferred *HTTPS Management Port* number and click *Update*. If you change the port number, you must log into the Firewall using the port number as well as the IP address. For example, if you change the port number to 700, you would log in using: **https://192.168.168.1:700**

The *HTTPS Management Certificate Common Name* defaults to the Firewall LAN port address. This allows you to continue using a certificate without downloading a new one each time you log into the Firewall.

Using the Firewall with the NBX Business Telephone System

3Com recommends that you place your NBX Processor on the LAN port of the Firewall. This is to ensure that your telephone system is completely secure from hackers on the Internet. If you wish to use NBX phones on the WAN or DMZ ports of the Firewall, then you must open a specific port on the Firewall. Do this by following these simple steps:

- 1 Access the Web interface from a Web browser.
- 2 Click *Policy*.
- 3 Click the *Add Service* tab.
- 4 Select *3Com NBX* for the Name of the service.
- 5 Click *Add*.
- 6 Click on the *Policy Rules* tab.
- 7 Click *Allow*, and select *3Com NBX* from the pull down menu.
- 8 Click *WAN* or *DMZ* for the Source and select *LAN* for the Destination.
- 9 Click *Update* and restart the Firewall.

8

ADVANCED SETTINGS

This chapter describes the commands and options available in the *Advanced* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click *Advanced* and then the appropriate tab.

The following sections are covered in this chapter:

- [Automatic Proxy/Webcache Forwarding](#)
- [Specifying Intranet Settings](#)
- [Setting Up Static Routes](#)
- [Setting up One-to-One NAT](#)
- [Configuring the Ethernet Port Settings](#)

Automatic Proxy/Webcache Forwarding

A proxy server intercepts all requests to the Web server to see if it can fulfill the requests by returning a locally stored copy of the requested information. If not, the proxy:

- Completes the request to the server
- Returns the requested information to the user
- Saves it locally to fulfill future requests

Because of this, a proxy can improve Internet response and lessen the load on the Internet link. For example, suppose a school is using the Internet for a research project. A student requests a certain Web page, and then sometime later, a second student requests the same page. Instead of forwarding the request to the Web server where the page resides, the proxy server returns the local copy of the page that it already fetched for the first student.

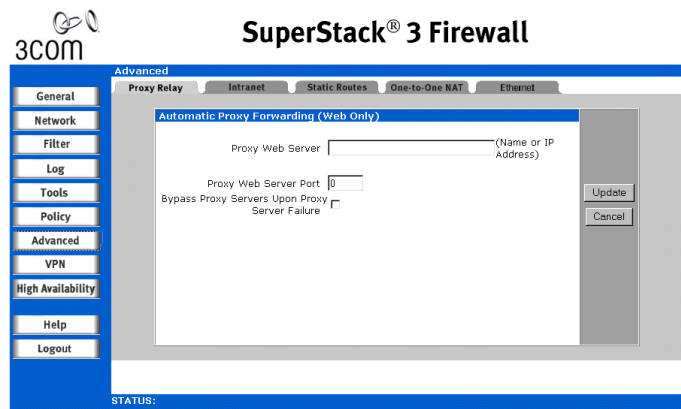
The problem with installing a proxy server on the LAN is that each client must be configured to support the proxy, which adds to administration tasks.

The alternative is to move the proxy to the WAN or DMZ, depending upon the level of protection desired, and enable Automatic Proxy Forwarding. The Firewall can automatically forward all Web proxy requests to the proxy server without client configuration. As a result, no client configuration is required when a Web Proxy is used.

The Firewall can also be used to forward all Web (HTTP) traffic to a Webcache on the network. The Webcache can be placed either on the WAN or the DMZ side of the Firewall. The installation is the same as for a Proxy Server. See below.

- 1 Click *Advanced*, and then select the *Proxy Relay* tab. A window similar to that in [Figure 54](#) displays.

Figure 54 Proxy Relay Window

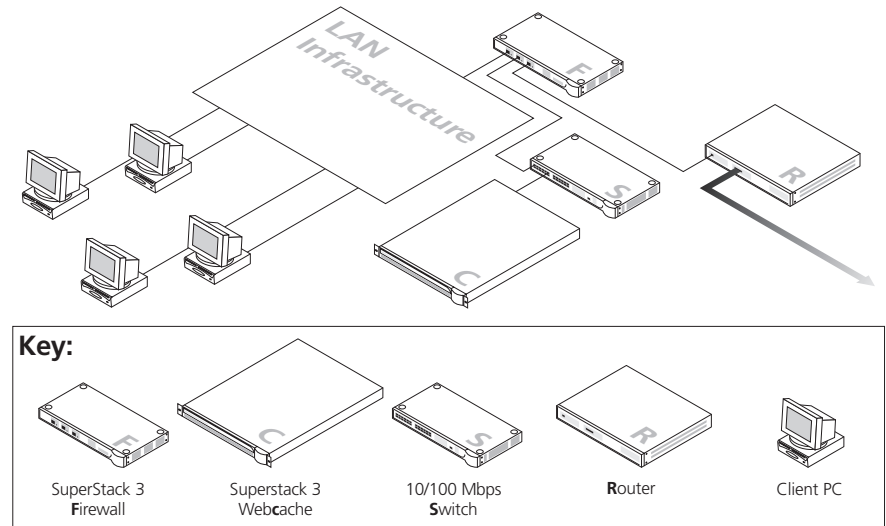


- 2 Enter the IP address of the proxy or webcache in the *Proxy Web Server Address* box, and the proxy's IP port in the *Proxy Web Server Port* box.
- 3 If you want to allow access to the Internet in the event of a proxy server failure, check the *Bypass Proxy Servers Upon Proxy Server Failure* check box.
- 4 Click *Update* to save your changes.

Deploying the SuperStack 3 Webcache as a Proxy of the Firewall

The following example describes how to install the 3Com SuperStack® 3 Webcache 1000/3000 (3C16115/3C16116) as a proxy server of the SuperStack 3 Firewall (3CR16110-95). A sample network layout is shown in [Figure 55](#).

Figure 55 Deploying the Firewall and Webcache together



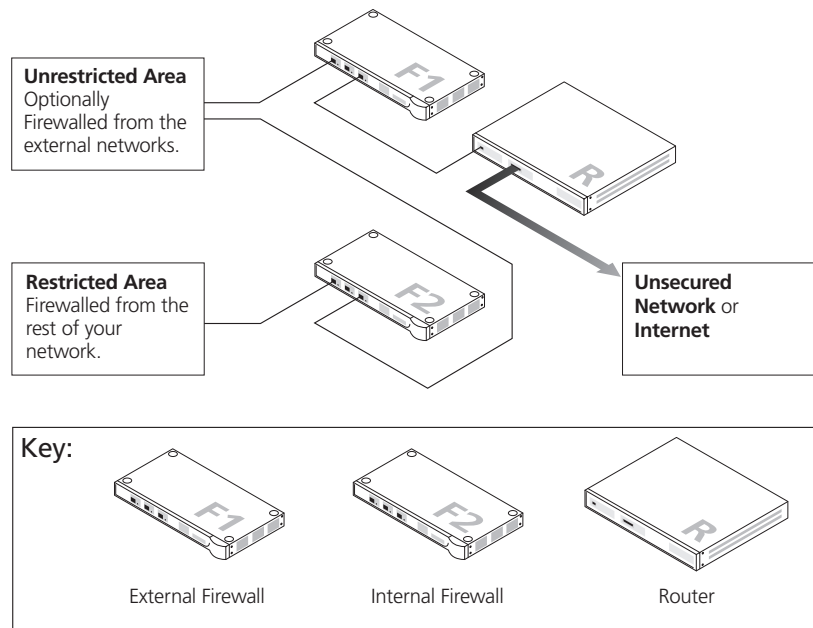
- 1 Install the Webcache as described in the Superstack 3 Webcache User Guide (DUA1611-5AAA0x) taking into account any safety information.
 - a Install the Webcache on a Hub or Switch connected to the DMZ port of the Firewall. Use the LAN port of the Webcache for this connection.
 - b Set the Webcache to *Proxy Mode* and not *Transparent Mode*. This setting can be made from the *Getting Started Wizard* or by selecting *Device View > System > Caching > Set Caching Mode* from the Web interface.
 - c In the *Port Number* field enter the number **8080** (this is the default value).
 - d You can use *Web Site Blocking* on either the Webcache or the Firewall.
- 2 Install the Firewall according to the Superstack 3 Firewall User Guide (this guide) taking into account any safety information.
 - a On the Web interface of the Firewall click *Advanced* then *Proxy Relay*.

- b** In the *Proxy Web Server Address* field enter the IP address of your Webcache.
 - c** In the *Proxy Web Server Port* field enter the number **8080**
 - d** Click *Update* to save your changes.
- 3** No configuration is necessary on the client machines. The Firewall intercepts any HTTP requests for external URLs and forwards the traffic to the Webcache.

Specifying Intranet Settings

In some cases, it is desirable to prevent access to certain resources by unauthorized users on the LAN. For example, a school's administration office may be placed behind the Firewall to restrict access to its computers by users in the Student Computer Lab. Similarly, an organization's accounting, research, or other sensitive resources may be protected against unauthorized access by other users on the same network. By default, protected LAN users can only access the Internet and no other devices between the WAN port and the Internet. To enable access to the area between the Firewall's WAN port and the Internet (referred to as the intranet), you must specify intranet settings for the Firewall.

To achieve internal firewalling, connect a second Firewall between the unrestricted and the restricted segments on the LAN, as shown in [Figure 56](#). In this diagram the Firewall labelled F2 is protecting an internal network.

Figure 56 Connecting the Firewall to protect an internal part of the network

Installing the Firewall to Protect the Intranet

The following describes how to install and configure the Firewall to provide intranet firewalling.

- 1 Connect the Ethernet port labeled LAN on the front of the Firewall to the network segment that will be protected against unauthorized access.
- 2 Connect the Ethernet port labeled WAN on the front of the Firewall to the rest of the network.

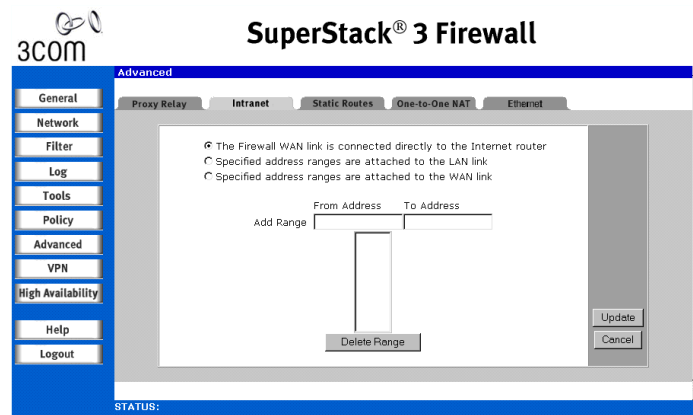


Devices connected to the WAN port do not have Firewall or Web Site Filter protection. It is advised that you use another Firewall to protect these computers.

- 3 Connect the power cord to the back of the Firewall and then connect to an AC power outlet.

Configuring the Firewall to Protect the Intranet

Click *Advanced*, and then select the *Intranet* tab. A window similar to that in [Figure 57](#) displays.

Figure 57 Intranet Window

To enable intranet firewalling, it is necessary to identify which machines are protected against unauthorized access by specifying the IP addresses of these machines. You can do this in two ways:

- Inclusively by specifying which machines are members of the segment with restricted access.
- Exclusively by specifying which machines are not members of the segment with the restricted access.

Using the inclusive method, you specify the IP addresses of the machines which are connected to the Firewall's LAN port. Use this method in cases such as a small accounting office in a large LAN, where it may be easier to identify the small number of machines with restricted access rather than the larger number of machines on the corporate network.

Using the exclusive method, you specify the IP addresses of the machines connected to the Firewall's WAN port. Use this method in cases such as a large school district with a small student computer lab where it would be easier to specify the small number of machines on the WAN which are not protected by the intranet Firewall, rather than the larger number of machines which are.

Typically, it is easier to enter the IP addresses from the smaller number of machines. Enter these addresses individually, or as a range.



IP addresses for Workstations on the LAN port must have static IP addresses or use the Internet Firewall as a DHCP server. It is not possible for them to use a DHCP server connected to the WAN port.

- *The Firewall WAN link is connected directly to the Internet router* — Use this setting if the Firewall is protecting the entire network. This is the default setting.

Click *Update* to save the configuration.

- *Specified address ranges are attached to the LAN link* — Select this when it is easier to specify which devices are on the LAN. If a machine's IP address is not specified, all communications through the Firewall for that machine are blocked.

Click *Update* to save the configuration.

- *Specified address ranges are attached to the WAN link* — Select this when it is easier to specify which devices are on the WAN port.

Click *Update* to save the configuration.

Add Range

To enter a range of addresses, such as the 51 IP addresses from **192.168.23.50** to **192.168.23.100**, type the starting address in the *From Address* box and the ending address in the *To Address* box. To specify an individual address, type it in the *From Address* box only. You can specify up to 64 address ranges.

Click *Update* to save the configuration.

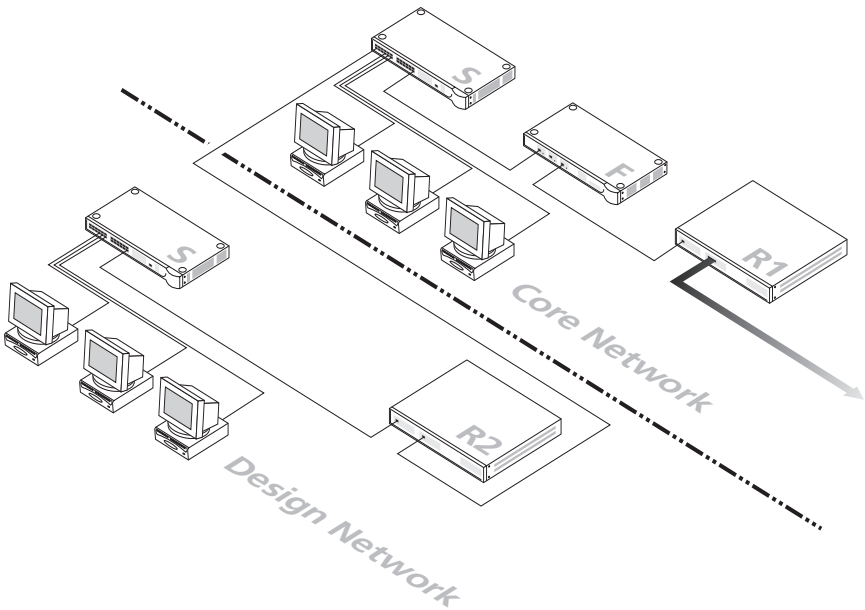
Setting Up Static Routes

If the network has internal routers, you must specify their addresses and network information.

Use static routes if the LAN, DMZ or WAN is segmented into subnets, either for size or practical considerations. For example, you can create a subnet which only contains an organization's graphic design shop, isolating it from traffic on the rest of the LAN.

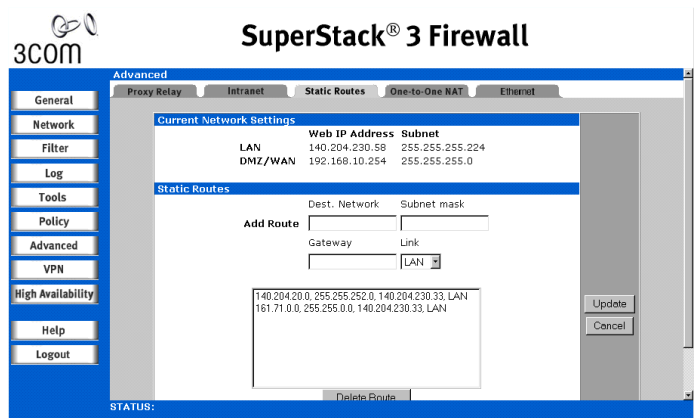
This example is shown in [Figure 58](#). Traffic on each network is separated. PCs on the design shop network communicate with PCs on the core network via router *R2*. PCs on the core network communicate with PCs on the design network via the Firewall *F* then the router *R2*.

Figure 58 Isolating a network using a second router



To configure static routes click *Advanced* and then select the *Static Routes* tab. A window similar to that in [Figure 59](#) displays.

Figure 59 Static Routes Window



LAN

The IP Address and Subnet on the Firewall's LAN port are shown. See [“Specifying the LAN Settings”](#) on [page 64](#) to change these settings.

DMZ/WAN

The IP addresses of the DMZ, if appropriate, and WAN ports are shown. These differ from that of the LAN port if NAT is enabled. See [“Specifying the WAN/DMZ Settings”](#) on [page 66](#) to change these settings.

Add Route

Type the destination network of the router in the *Dest. Network* box, and the IP address of the router as it appears on Firewall’s subnet in the *Gateway* box. From the Link drop-down list, select the port on the Firewall, *LAN*, *DMZ* or *WAN*, that the router is connected to. You may have to check the configuration of the LAN routers in order to find this information.

Click *Update* to send the configuration data to the Firewall.

Setting up
One-to-One NAT

One-to-One NAT creates a relationship which maps valid external addresses to internal addresses hidden by NAT. Machines with an internal address may be accessed at the corresponding external valid IP address.

To create this relationship between internal and external addresses, define internal and external address ranges of equal length. Once you have defined that relationship, the machine with the first internal address is accessible at the first IP address in the external address range, the second machine at the second external IP address, and so on.

Consider a LAN for which the ISP has assigned the IP address range from 209.19.28.16 to 209.19.28.31, with 209.19.28.16 used as the NAT Public Address. You have configured the address range of 192.168.1.1 to 192.168.1.255 to be used for the machines on the LAN. Typically, only machines that have been designated as Public LAN Servers are accessible from the Internet. However, with One-to-One NAT, the machines with the internal IP addresses of 192.168.1.2 to 192.168.1.16 can be made accessible at the corresponding external IP address, as shown in [Table 4](#).

Table 4 Address Correspondence in One-to-One NAT

LAN Address	Corresponding WAN Address	Accessed Through
192.168.1.1	209.19.28.16	Inaccessible: Firewall WAN IP Address
192.168.1.2	209.19.28.17	209.19.28.17

Table 4 Address Correspondence in One-to-One NAT

LAN Address	Corresponding WAN Address	Accessed Through
[...]	[...]	[...]
192.168.1.16	209.19.28.31	209.19.28.31
192.168.1.17	No corresponding valid IP address	Inaccessible except as Public LAN Server
[...]	[...]	[...]
192.168.1.255	No corresponding valid IP address	Inaccessible except as Public LAN Server



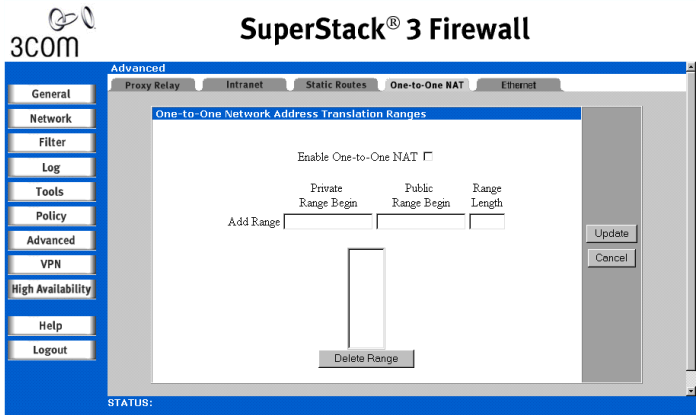
You cannot include the Firewall WAN IP Address in a range.

To set up One-to One NAT click *Advanced*, and then select the *One-to-One NAT* tab. A window similar to that in [Figure 60](#) displays.



Ensure that NAT is enabled on the LAN or DMZ before configuring One-to-One NAT. See [“Setting the Network Addressing Mode”](#) on [page 63](#) for details about the LAN See [“Specifying DMZ Addresses”](#) on [page 67](#) for details of NAT in DMZ.

Figure 60 One-to-One NAT Window



Private Range Begin

Type the beginning IP address of the private address range being mapped in the *Private Range Begin* box. This is the IP address of the first machine being made accessible from the Internet.



Do not include the Firewall WAN IP Address in any range.

Public Range Begin

Type the beginning IP address of the public address range being mapped in the *Public Range Begin* box. This address is assigned by the ISP.

Range Length

Type the number of IP addresses for the range. The range length may not exceed the number of valid IP address. You can add up to 64 ranges. To map a single address, use a *Range Length* of 1.

Click *Update* to save changes. Restart the Firewall for changes to take effect.



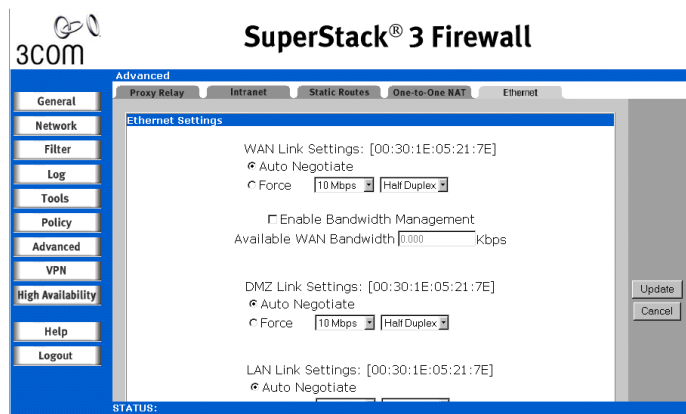
One-to-One NAT does not change the way the Firewall functions work. Access to machines on the LAN from the Internet is not allowed unless you have set up Network Access Rules, or established Authenticated User sessions.

Configuring the Ethernet Port Settings

This option allows you to configure the Ethernet Port settings for the LAN, WAN and DMZ ports. This option is useful if the devices you are connecting to these ports are unable to auto-negotiate the connections.

Click *Advanced* and then click the Ethernet tab to display the screen shown in [Figure 61](#).

Figure 61 Ethernet Window



Ethernet Settings

Use the *Ethernet Settings* options to assign the port type for the LAN, DMZ, and WAN ports on your Firewall. By default, the Firewall *auto-negotiates* the port type based on the network devices connected to it. You can override the default settings and force the Firewall to the appropriate Ethernet speed for your network. You may also configure the Ethernet settings for *Full Duplex* or *Half Duplex* mode.



3Com recommends that you use autonegotiation unless there are speed or duplex mode issues. If you manually override the Firewall interface's autonegotiate setting, then the device attached to the interface must also be manually set to the same Ethernet settings.

Bandwidth Management on the WAN port

You can implement Bandwidth Management on outbound traffic on the Firewall. Before you enable this function you must know the bandwidth of your connection in Kbps and you must understand how bandwidth management works. For an overview of this function, see [“Bandwidth Management”](#) on [page 228](#).

If you want to use Bandwidth Management, check the *Enable Bandwidth Management* box and enter the available bandwidth in Kbps.

Once you have enabled bandwidth management, you can configure Rules to use bandwidth management.



CAUTION: *Bandwidth management is very complex and requires extensive knowledge of networks and networking protocols. Incorrect bandwidth management can cause network problems or degradation of network performance.*

Proxy Management Workstation Ethernet address on WAN

If this check box is selected, the WAN address of the Firewall assumes the Ethernet address of the computer that you use to login and manage the Firewall. This option should be selected if your ISP only provides Internet access to devices with predetermined Ethernet addresses. Do not select this option if you manage the Firewall from a workstation on the WAN or DMZ.

MTU Settings

You can set the MTU (Maximum Transmission Unit) for IP packets that are sent through the Firewall. If large IP packets are sent through the Firewall, these packets may be dropped or fragmented by a router unable to handle large packet sizes. If the maximum packet size is too small, a large

percentage of IP bandwidth is allocated to packet header data and more TCP/IP acknowledgements will need to be sent and processed. The default value, determined by the Ethernet standard MTU, is 1500 octets. The minimum value that can be set is 68. Decreasing the packet size may improve the performance of the network. The *MTU* value must be a multiple of 8 bytes plus 20 bytes for the IP header.

9

CONFIGURING VIRTUAL PRIVATE NETWORK SERVICES

This chapter describes the commands and options available in the *VPN* menu. The menu is broken up into sections shown in the user interface as tabs. To access a command click on *VPN* and then on the appropriate tab.

The following sections are covered in this chapter:

- [Editing VPN Summary Information](#)
- [Configuring a VPN Security Association](#)
- [Configuring the IRE VPN Client for use with the Firewall](#)
- [Using Third Party Digital Certificates](#)
- [Configuring the Firewall for use with Local Certificates](#)
- [Configuring the Firewall for use with CA Certificates](#)
- [Configuring a VPN Security Association using IKE and a Third Party Certificate](#)
- [Configuring the Firewall as an L2TP Server](#)

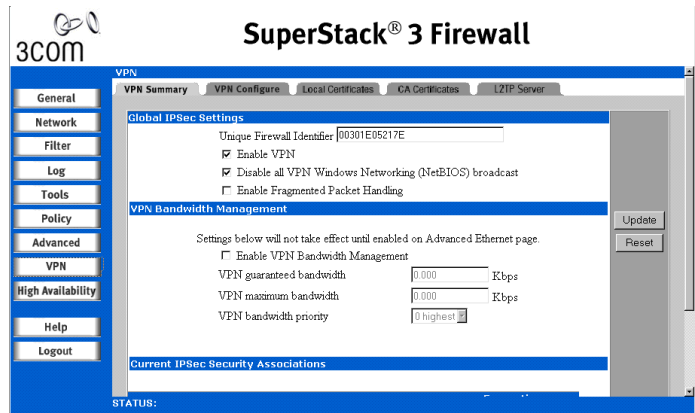


Before configuring VPNs for the first time, 3Com recommends you read [“Virtual Private Network Services”](#) on [page 221](#) which provides an overview of how VPNs work and the different configuration options.

Editing VPN Summary Information

To view the VPN Summary click on *VPN* and then select the *VPN Summary* tab. A window similar to that in [Figure 62](#) displays.

Figure 62 VPN Summary Window



Changing the Global IPSec Settings

The Firewall's security uses the IPSec protocol to transmit encrypted data. The settings in the *Current IPSec Settings* section affect all traffic transmitted across the Firewall.

Unique Firewall Identifier

The *Unique Firewall Identifier* is used to identify the Firewall within a network. To change the value enter a string of numbers and letters in the *Unique Firewall Identifier* field and click *Update*. The *Unique Firewall Identifier* defaults to the serial number of the Firewall.



CAUTION: The Unique Firewall Identifier must be different for each Firewall within your network as VPN connections may refer to Firewalls by name.

Enable VPN

To enable VPN connections check the *Enable VPN* box and click *Update*. If VPN is disabled the VPN settings are visible on screen and can still be amended but have no effect until VPN is enabled.

Disable all VPN Windows Networking (NetBIOS) Broadcasts

NetBIOS broadcasts are used when Windows PCs browse their local network. Disabling NetBIOS broadcasts stops Windows PCs from being able to browse networks on other sites that are connected by the Firewall but has no effect on browsing the local site or making connections between sites.

Check the [Disable all VPN Windows Networking \(NetBIOS\) Broadcasts](#) check box to disable NetBIOS traffic. Click *Update* to save your changes.

Enable Fragmented Packet Handling

Check the *Enable Fragmented Packet Handling* box to allow the Firewall to reduce that packet size when communicating with other Firewalls. Enable this check box if “Fragmented IPSec packet dropped” messages appear in the Event Log. Click *Update* to save your changes.

Configuring VPN Bandwidth Management

The Firewall can be configured for bandwidth management of outbound (WAN) network traffic using the bandwidth management options. Before you can enable and configure bandwidth management for VPNs, you must enable it on the *Ethernet* tab that you can select from the *Advanced* menu. See [“Configuring the Ethernet Port Settings”](#) on [page 147](#) for more information.



CAUTION: *Bandwidth management is very complex and requires extensive knowledge of networks and networking protocols. Incorrect bandwidth management can cause network problems or degradation of network performance. See [“Bandwidth Management”](#) on [page 228](#) for an overview of this function.*



You can only configure bandwidth management for all VPNs and not for individual VPN SAs.

Enable VPN Bandwidth Management

Check this box if you want to enable bandwidth management for all VPN Security Associations.

VPN Guaranteed Bandwidth

Enter the *Guaranteed Bandwidth* in Kbps.

VPN Maximum Bandwidth

Enter the *Maximum Bandwidth* in Kbps.

VPN Bandwidth Priority

Set the *Bandwidth Priority* for VPN traffic where 0 is highest and 7 lowest.

Viewing the Current IPSec Security Associations

The *Current IPSec Security Associations* section of the *VPN Summary* screen shows all Security Associations (SAs) that have been created in the *VPN Configure* window. The *Name* listed in the summary table links to the corresponding VPN configuration.

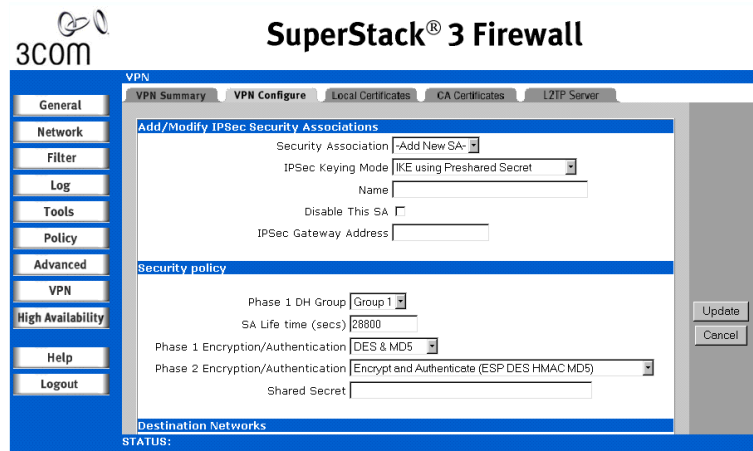
A *Renegotiate* option appears next to an IKE VPN Security Association when the VPN connection is active. Click *Renegotiate* to initiate the VPN handshake and the exchange of new encryption and authentication keys.

Configuring a VPN Security Association

The SuperStack 3 Firewall supports up to 1001 Security Associations. Of these SAs, 1000 support a single site-to-site or client VPN tunnel, while the remaining single SA can support up to 1000 concurrent client VPN tunnels. This is called the *GroupVPN* SA. If you only have VPN client connections, you need only use the GroupVPN SA. However you will need to configure a separate SA for each site-to-site connection

To configure the VPN Security Associations click on *VPN* and then select the *Configure* tab. A window similar to that in [Figure 63](#) displays.

Figure 63 VPN Configure Window



Adding/Modifying IPSec Security Associations

To add a new Security Association (SA) click the drop down box labelled *Security Associations* and select the option labelled *Add New SA*. Set up the new SA using the options below. Click *Update* to save your changes.

To modify a SA click the drop down box labelled *Security Associations* and select the SA you want to modify. Change the SA using the options below. When you have completed your changes click *Update* to save your changes.

To delete an SA click the *Security Association* drop down box and select the SA you want to delete. Click *Delete* to delete the SA.



The GroupVPN Security Association cannot be deleted.

IPSec Keying Mode

To select the keying mode click on the *IPSec Keying Mode* drop down box and select one of the options.

- *IKE Using pre-shared secret* (Internet Key Exchange using pre-shared Secret) is the default keying mode and offers more security than a *Manual Key*.
- *IKE Using 3rd Party Certificates* offers the highest level of security but requires the configuration of CA and Local Certificates. See [“Using Third Party Digital Certificates”](#) on [page 169](#) for more information.
- *Manual Key* does not offer as high a level of security as IKE but is compatible with a wider range of VPN devices.

This option is not available when using *GroupVPN*.

SA Name

Enter a descriptive name for the Security Association in the *SA Name* field. This allows you to identify the link for which this Security Association was created.

The *SA Name* field is not available when using *GroupVPN*.

Disable This SA

Check the *Disable this SA* box to temporarily disable a Security Association. The association is not deleted but ceases to function until the box is unchecked.

IPSec Gateway Address

Enter the address of the target of the VPN link in the *IPSec Gateway Address* field. This is typically the address of another Firewall or a remote client. If the client does not have a fixed IP address leave this field blank or set to 0.0.0.0.

This field is not applicable when using *GroupVPN* and should be left blank or set to 0.0.0.0 if you are setting up a SA for VPN clients which do not have a fixed IP address.

Security Policy Settings for IKE using Pre-Shared Secret

The options in the *Security policy* area of the screen relate to the current Security Association being created/modified. A description of each option is listed below.

Phase 1 DH Group

Diffie-Hellman (DH) key exchange (a key agreement protocol) is used during phase 1 of the authentication process. Select from one of three settings:

Table 5 DH Groups

Group Descriptor	Prime Size (bits)	When to use...
Group 1	768	When network speed is important.
Group 2	1024	When a compromise between network speed and network security is required.
Group 5	1536	When network security is important.

SA Life time (secs)

The [SA Life time \(secs\)](#) field allows you to specify the number of seconds you want a Security Association to last before new encryption and authentication keys must be exchanged.

As the connection is temporarily disabled when the keys are renegotiated, a low value (short time) increases security but may cause inconvenience. The default value for the [SA Life time \(secs\)](#) field is 28800 seconds (8 hours). Enter the number 28800 or your desired value.

Phase 1 Encryption/Authentication

You can select an encryption method for the VPN tunnel. There are four options:

- DES & MD5
- DES & SHA1
- 3DES & MD5
- 3DES & SHA1

These are listed in order from least secure to most secure. If network speed is preferred, then select *DES & MD5*. If network security is preferred, then select *3DES & SHA1*. To compromise between network speed and network security, then select *DES & SHA1*.

Phase 2 Encryption/Authentication

Each encryption method is described in [Table 6](#) on [page 159](#). However, *Phase 2 Encryption/Authentication* is different for the *Group VPN SA*. The

VPN client does not support ArcFour encryption methods and you cannot disable encryption in the VPN client. The following four methods are the only ones available for the *Group VPN SA* and are listed in order from most secure to least secure.

- *Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)*
- *Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)*
- *Strong Encrypt and Authenticate (ESP DES HMAC SHA1)*
- *Strong Encrypt and Authenticate (ESP DES HMAC MD5)*

Shared Secret

A shared secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE SA. This field can be any combination of alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Precautions should be taken when delivering/exchanging this shared secret to assure that a third party cannot compromise the security of a VPN tunnel.

Enter your chosen shared secret in the *Shared Secret* field.

Security Policy Settings for IKE Using 3rd Party Certificates

The security policy settings are the same as for *IKE using Pre-Shared Secret* except that there is *Certificate ID* Field. See the section above for an explanation of the fields in this section. Once you have completed these fields you must enter the Peer Certificates ID. See [“Peer Certificate's ID”](#) on [page 161](#) for more information.

Security Policy Settings using Manual Key

The options in the *Security policy* area of the screen change if you select *Manual Key*. A description of each option is listed below.

Incoming SPI and Outgoing SPI

The *Incoming Security Parameter Index (SPI)* and *Outgoing SPI* are two eight digit hexadecimal numbers that identify the Security Association used for the VPN Tunnel. The *Incoming SPI* and *Outgoing SPI* for a SA can be the same but must differ for all other SPIs used on your network

Additionally the values from 00000000 to 000000FF have been reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI.

Enter your chosen *Incoming SPI* and *Outgoing SPI* in the relevant fields.



If you enter less than eight hexadecimal digits the SPI is padded with leading zeros. For example SPIs of "F00" and "00000F00" are treated as equivalent.

The *Incoming SPI* and *Outgoing SPI* are only used when *Manual Keying* is employed. These fields do not appear when using IKE as your *IPSec Keying Mode*. Incoming SPI must match Outgoing SPI and on the remote device or VPN client. Outgoing SPI must match Incoming SPI on the remote device or client.

Encryption Method

The Firewall supports fifteen encryption methods for establishing a VPN tunnel. These are shown in [Table 6](#) on [page 159](#).

Encryption Key

The *Encryption Key* is a hexadecimal number that is used to encrypt the VPN tunnel when using *Manual Keying*. The length of the *Encryption Key* is determined by the method of encryption that is used.

- For 56 bit DES the number must be 16 hexadecimal digits long.
- For 56 bit ARC4 the number must be 16 hexadecimal digits long.
- For 168 bit 3DES the number must be 48 hexadecimal digits long.

If the *Encryption Key* is less than the value stated above it is rejected by the Firewall. If it is longer than stated, then the number is truncated and the stated number of digits used.

The *Encryption Key* is only used when *Manual Keying* is employed. This field does not appear when using IKE as your *IPSec Keying Mode*. Encryption keys are automatically created when using IKE.

Authentication Key

The *Authentication Key* is a hexadecimal number that is used to authenticate the users of the VPN tunnel when using *Manual Keying*. The length of the *Authentication Key* is always 32 digits.

If the *Authentication Key* is less than the value stated above it is rejected by the Firewall. If it is longer than stated then the number is truncated.

Encryption Methods

Table 6 Firewall Encryption Methods

Method	Speed	Security	Supported by
<i>Tunnel Only (ESP NULL)</i> provides no encryption or authentication but can be used to access machines at private addresses behind NAT. Can also be used to allow unsupported protocols through the Firewall.	Very Fast	Low	Manual Key, IKE
<i>Encrypt (ESP DES)</i> uses 56 bit DES to provide an encrypted VPN tunnel. Security professionals consider DES to be a secure encryption method.	Fast	High	Manual Key, IKE
<i>Fast Encrypt (ESP ARCFour)</i> uses 56 bit ARCFour to provide an encrypted VPN tunnel. ARCFour is widely considered to be a secure encryption method, and will have more impact on the throughput of the firewall than DES. As a result, this encryption method is recommended for compatibility with third party devices only.	Medium	Medium	Manual Key, IKE
<i>Strong Encrypt (ESP 3DES)</i> uses 168 bit 3DES to provide an encrypted VPN tunnel. Security professionals consider 3DES to be an very secure encryption method.	Fast	Extremely High	GroupVPN, Manual Key, IKE
<i>Strong Encrypt and Authenticate (ESP 3DES HMAC MD5)</i> Tunnel and Triple DES Encrypt with MD5 Authentication. This method uses 168 bit 3DES as the encryption method and HMAC MD5 Authentication. Security professionals consider 3DES to be a very secure encryption method.	Fast	Extremely High	GroupVPN, Manual Key, IKE
<i>Strong Encrypt for Checkpoint (ESP 3DES)</i> Triple DES Encrypt. This method uses 168 bit 3DES as the encryption method. Security professionals consider 3DES to be a very secure encryption method. This method will provide interoperability with Check Point FireWall-1.	Fast	Extremely High	Manual Key, IKE (for Checkpoint only)

Table 6 Firewall Encryption Methods

Method	Speed	Security	Supported by
<i>Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)</i> Tunnel and Triple DES Encrypt with MD5 Authentication. This method uses 168 bit 3DES as the encryption method and HMAC SHA1 Authentication. Security professionals consider 3DES to be a very secure encryption method.	Fast	Very High	GroupVPN, Manual Key, IKE
<i>Encrypt for Check Point (ESP DES rfc1829)</i> uses 56 bit DES as specified in RFC 1829 to provide an encrypted VPN tunnel. This method will provide interoperability with other IPsec VPN gateways, such as Check Point FW-1.	Fast	High	Manual Key, IKE, Check Point FW-1
<i>Encrypt and Authenticate (ESP DES HMAC MD5)</i> uses 56 bit DES to encrypt and HMAC MD5 to authenticate the VPN tunnel.	Fast	Very High	GroupVPN, Manual Key, IKE
<i>Authenticate (AH MD5)</i> provides an unencrypted but authenticated VPN tunnel. This method uses an Authentication Header (AH) to authenticate the data.	Very Fast	Low	Manual Key, IKE
<i>Authenticate (AH SHA1)</i> provides an unencrypted but authenticated VPN tunnel. This method uses an Authentication Head (AH) and SHA1 to authenticate the data and will have minor impact on the data throughput of Firewall.	Very Fast	Low	Manual Key, IKE
<i>Authenticate (ESP MD5)</i> provides an unencrypted but authenticated VPN tunnel. This method uses ESP MD5 to authenticate the data and will have minor impact on the data throughput of Firewall.	Very Fast	Low	Manual Key, IKE
<i>Authenticate (ESP SHA1)</i> provides an unencrypted but authenticated VPN tunnel. This method uses ESP SHA1 to authenticate the data and will have minor impact on the data throughput of Firewall.	Very Fast	Low	Manual Key, IKE

Table 6 Firewall Encryption Methods

Method	Speed	Security	Supported by
<i>Encrypt and Authenticate (ESP DES HMAC SHA1) Tunnel, Encrypt, and Authenticate.</i> This method uses 56 bit DES as the encryption method, and authenticates the data using HMAC SHA	Fast	High	GroupVPN, Manual Key, IKE

Select your preferred method from the [Encryption Method](#) drop-down box. 3Com recommends that you use DES or 3DES and SHA1 for security. Use ArcFour where compatibility with third party products is required.

3DES is only available with the 168 bit version of the Firewall's firmware. See <http://www.3Com.com/ssfirewall> for information about obtaining this version of the firmware.

Peer Certificate's ID

This section is only available if the *IKE Using 3rd party Certificates* option has been selected. Select the *ID Type*. You can select *Distinguished Name*, *E-mail ID* or *Domain Name* from the menu. Then cut and paste the information from the Local Certificate into the text field.

Use the SA as the default route for all Internet traffic

This option is available for Security Associations using IKE, and Manual Key. Enable this check box if you want all remote VPN connections to access the Internet through this SA. You can only configure one SA to use this setting.

Destination network obtains IP addresses using DHCP through this SA

This option is available for Security Associations using IKE but not Group VPN. Enable this checkbox to be able to centrally manage your IP address allocation.

Setting the Destination Network for the VPN Tunnel

For a site-to-site link you need to configure a Security Association with the IP subnet that is connected to the LAN port of the remote Firewall. This allows the Firewall to route the packets appropriately over the VPN tunnel. The remote Firewall also needs to be configured in a similar way using the local Firewall's LAN IP subnet for its destination network.

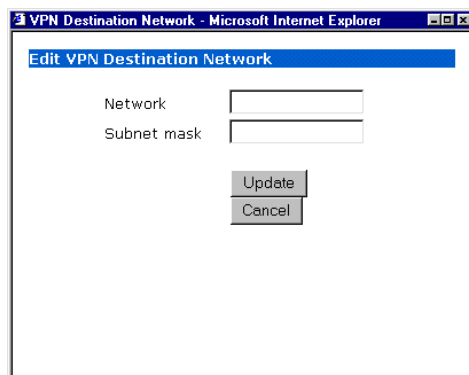
If you are configuring an SA for an individual remote PC client, configure the destination network as the internal IP address of the client and use a

subnet mask of 255.255.255.255. See [“Configuring the IRE VPN Client for use with the Firewall”](#) on [page 166](#) for more information.

Adding a New Network

To add a new network range click *Add New Network* to open the dialog box shown in [Figure 64](#).

Figure 64 Add New Network dialog



Enter the network address and subnet mask for the network you want to add in the dialog box displayed.

Deleting a Network

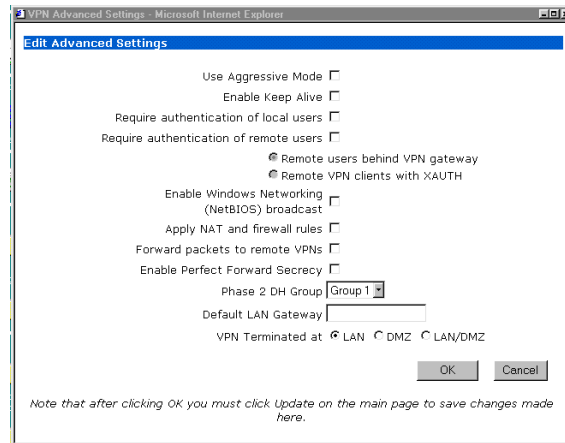
To delete a network click the trash can icon next to the network you want to delete and confirm your decision when asked.

Editing a Network Range

To edit a network click the pencil and paper icon next to the range you want to edit. Change the network settings to the desired values and click *Update*.

Advanced Settings for VPNs

To access all the Advanced Settings for a VPN SA, click *Configure* and then select the SA from the drop-down menu. Click *Advanced Settings* to display the screen shown in [Figure 65](#) which opens in a separate window.

Figure 65 Advanced Settings Window

Use Aggressive Mode

Aggressive Mode forces the Firewall to establish the VPN tunnel even if the Firewall has a static IP address.

Enable Keep Alive

Check this box to allow the VPN tunnel to remain active and maintain its current connection by listening for traffic on the network segment between the two connections. Interruption of the signal forces the tunnel to renegotiate the connection.

Require authentication of local users

Check this box if you require all outbound VPN traffic on this SA to be from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

Require authentication of remote users

Check this box if you require all inbound VPN traffic on this SA to be from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. Select *Remote users behind VPN gateway* if remote users have a VPN tunnel that terminates on the VPN gateway. Select *Remote VPN clients with XAUTH* if remote users require authentication using XAUTH and are accessing the Firewall via a VPN client.

Enable Windows Networking (NetBIOS) broadcast

Computers running Microsoft Windows® communicate with each other through NetBIOS broadcast packets. Check this box to access remote network resources by browsing the Windows Network Neighborhood.

Apply NAT and firewall rules

This option allows a remote site's LAN to be hidden from the corporate site. It is useful when a remote office's network traffic is initiated to the corporate office. The IPSec tunnel is located between the Firewall WAN interface and the LAN segment of the corporate office. To protect the traffic, NAT (Network Address Translation) is performed on inbound packets when they are received. By using NAT for a VPN connection, computers on the remote LAN are viewed as one address (the Firewall public address) from the corporate LAN.



You cannot use this feature if you have Route all internet traffic through this SA enabled.



Offices can have overlapping LAN IP ranges if this option is selected.

Forward packets to remote VPNs

This option allows the remote VPN tunnel to participate in the Firewall's routing table. Inbound traffic is decrypted and can now be forwarded to a remote site through another VPN tunnel. Normally, inbound traffic is decrypted and only forwarded to the Firewall's LAN port or a specific route on the LAN that you have already configured on the *Routes* tab in the *Advanced* menu.

This feature allows you to create a *hub and spoke* network configuration by forwarding inbound traffic to a remote site over a VPN security association. Enable this option for each Security Association to create a hub and spoke network. Traffic then passes from a branch office to a branch office through the corporate office and you do not need to configure branch office to branch office VPNs.

Enable Perfect Forward Secrecy

Use this option to increase the renegotiation time of the VPN tunnel. This prevents a hacker using brute force to break encryption keys from obtaining other or future IPSec keys. During the Phase 2 renegotiation between two Firewalls or a Group VPN SA, an additional Diffie-Hellman (DH) key exchange is performed. *Enable Perfect Forward Secrecy* adds incremental security between gateways.

Phase 2 DH Group

If *Enable Perfect Forward Secrecy* is enabled, you can select the type of DH Key exchange (a key agreement protocol) to be used during Phase 2 of the authentication process to establish pre-shared keys. You can select from three well-known DH groups.

Table 7 DH Groups

Group Descriptor	Security	Prime Size (bits)
1	less secure	768
2	more secure	1024
5	most secure	1536

If network connection speed is an issue, select *Group 1*. If network security is an issue, select *Group 5*. To compromise between speed and security, select *Group 2*.

Default LAN Gateway

A Default LAN Gateway is used at a central site in conjunction with a remote site using the Route all internet traffic through this SA check box. Enter the IP address of the default LAN route for IPSec packets for this SA.

Incoming packets are decoded by the Firewall and compared to static routes configured in the Firewall. Since packets can have any destination IP address, it is impossible to configure enough static routes to handle the traffic. For packets received through an IPSec tunnel, the Firewall looks up the route for the LAN port. If no route is found, the Firewall checks for a *Default LAN Gateway*. If the *Default LAN Gateway* is found, the packet is routed through the gateway. Otherwise, the packet is dropped.

VPN Terminate at LAN, DMZ or LAN/DMZ

This option allows you to terminate a VPN tunnel at a specific destination instead of on the Firewall network. If you terminate the tunnel at a specific destination, the VPN tunnel has access to a specific portion of the LAN port or DMZ Port network.

Configuring the IRE VPN Client for use with the Firewall

This section covers the configuration of the Firewall VPN capability and the installation of the IRE VPN Client Software. There are several parts to this process:

- [Setting up the GroupVPN Security Association](#)
- [Installing the IRE VPN Client Software](#)
- [Configuring the IRE VPN Client](#)



If you are using Windows XP, do not use the IRE VPN Client. You must use the Windows VPN client and configure the Firewall to use the L2TP server. See [“Configuring the Firewall as an L2TP Server”](#) on [page 176](#) for more information.

Setting up the GroupVPN Security Association

To set up a Group VPN Security association, carry out the following:

- 1 Click *VPN* and then *Summary*.
 - a Ensure that *Enable VPN* is checked.
 - b Click *Update* to save any changes you have made.
- 2 Click *Configure*.
 - a Select *GroupVPN* from the *Security Association* drop-down box.
 - b Select *IKE using pre-shared secret* from the *IPSec Keying Mode* drop-down box
 - c Ensure that the *Disable This SA* box is not checked.
- 3 If you want to use a RADIUS server to authenticate users check the *Require XAUTH/RADIUS* box in the *Advanced Settings* and set up the Firewall for a RADIUS server as detailed in [“Configuring the Firewall to use a RADIUS Server”](#) on [page 127](#).
- 4 If you do not have a RADIUS server or do not wish to use your RADIUS server to authenticate users ensure that the *Require XAUTH/RADIUS* check box is not ticked.
- 5 Set the *SA Life time (secs)* field to 28000.
- 6 If you want extremely high security select the *Strong Encrypt and Authenticate* option from the *Encryption Method* drop-down box otherwise select *Encrypt and Authenticate*.

- 7 Enter an alphanumeric string of up to 30 characters into the *Shared Secret* field. As the security of your VPN tunnel depends on the shared secret pick something that cannot easily be guessed such as a string of numbers and letters.
- 8 Click *Export* and save the resulting file to a safe place. Consider this file as one of the keys to your network and keep it in a safe and private place.
- 9 Click *Update* to save the changes you have made.

Installing the IRE VPN Client Software

To install the IRE VPN Client Software on your computers:

- 1 Insert the CD that came with the Firewall into your CD-ROM Drive.
- 2 Go to the *VPN CLIENT* directory on the CD.
- 3 Double-click *setup.exe* and follow the VPN client Setup program's step-by-step instructions. This product does not require any serial key for installation.
- 4 Restart your computer after the VPN client Setup program has finished installing.

Configuring the IRE VPN Client

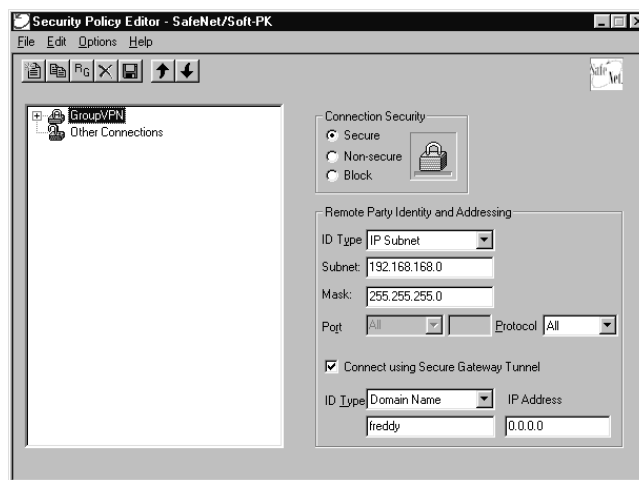
To configure the VPN Client:

- 1 Copy the previously saved export file (created in ["Setting up the GroupVPN Security Association"](#)) to a floppy disk or to the hard drive of the client machine.
- 2 Start the Safenet Security Policy Editor. To start the Security Policy Editor either select it from the *SafeNet Soft-PK* submenu of the Windows *Start* menu or double-click the *SafeNet* icon in the toolbar. A window similar to [Figure 66](#) is displayed.
- 3 Click on the *File* menu and select *Import Security Policy*.
- 4 Select the exported security file and click *Open*.
- 5 Close the *Security Policy Editor* saving changes when prompted.
- 6 Delete the export file from the hard drive if it was previously copied there.
- 7 Click the + sign next to Group VPN to reveal two sections.
- 8 Select *My Identity* to view the settings.
- 9 Click *Pre-Shared Key* to enter the Pre-Shared Secret. Click *OK*.

- 10 In the *Internet Interface* box, select the adapter used to access the Internet. Select *PPP Adapter* in the *Name* menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable, ISDN, or DSL line.
- 11 Click *File*, then *Save Changes* to save the settings to the security policy.

The client is now set up to access your network safely across the Internet.

Figure 66 Importing a saved *Security Policy*



Setting up L2TP Clients

Although PPTP is currently the most deployed client VPN protocol (natively supported by Windows prior to Windows 2000), L2TP over IPSec is becoming the de facto client VPN tunnelling mechanism due to its much improved security and standards-based interoperability.

Microsoft is promoting L2TP/IPSec as the standard VPN client and introduced both IPSec support and L2TP in Windows 2000 as separate components. Windows XP provides an integrated L2TP/IPSec client. Microsoft has also released a free integrated L2TP/IPSec client for Windows 98, NT and ME. (NOTE: not Windows 95).

Version 6.3.0 of the SuperStack 3 Firewall firmware supports an L2TP/IPSec server and can make use of the Microsoft L2TP/IPSec clients.

Unfortunately, each of these clients is configured differently and new clients are likely to appear in rapid succession. 3Com therefore provide

this information through the website. Use your browser to navigate to <http://www.3com.com/ssfirewall> and follow the *Documentation* link. The document *L2TP/IPSec Client Configuration* contains the information needed to set up L2TP clients.

Using Third Party Digital Certificates

This section provides an overview of how to use third party digital *Local Certificates* and *Certificate Authority (CA) Certificates* to verify the identity of trusted third parties. 3Com suggest you read this section and the following sections, before configuring your Firewall to use third party digital certificates:

- [Configuring the Firewall for use with CA Certificates](#)
- [Configuring the Firewall for use with Local Certificates](#)
- [Configuring a VPN Security Association using IKE and a Third Party Certificate](#)



This section assumes you are familiar with Public Key Infrastructure (PKI) and the implementation of digital certificates with VPN.

Overview

The Firewall supports third party certificates. Experience of implementing Public Key Infrastructure (PKI) is beneficial in order to understand the key components of digital certificates.

Internet Key Exchange (IKE) is an important part of IPSec VPN solutions and it can use digital signatures to authenticate peer devices before setting up security associations. Without digital signatures, VPN users must authenticate manually by exchanging shared secrets or symmetric keys. Devices using digital signatures do not require configuration changes every time a new device is added to the network.

The Firewall uses X.509 v3 as its certificate form and CRL v2 for its certificate revocation list. The Firewall supports CA Certificates from the following vendors:

- VeriSign
- Entrust

Third Party Digital Certificate Support

X.509 Version 3 Certificate Standard

The X.509 v3 certificate standard is a specification used with cryptographic certificates and allows you to define extensions which you

can include with your certificate. The firewall implements this standard in its third party certificate support. You can use a certificate signed and verified by a third party CA to use with a VPN SA.

A typical certificate consists of two sections: a data section and a signature section. The data section contains information such as the version of X.509 supported by the certificate, a certificate serial number, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA and the CA digital signature.

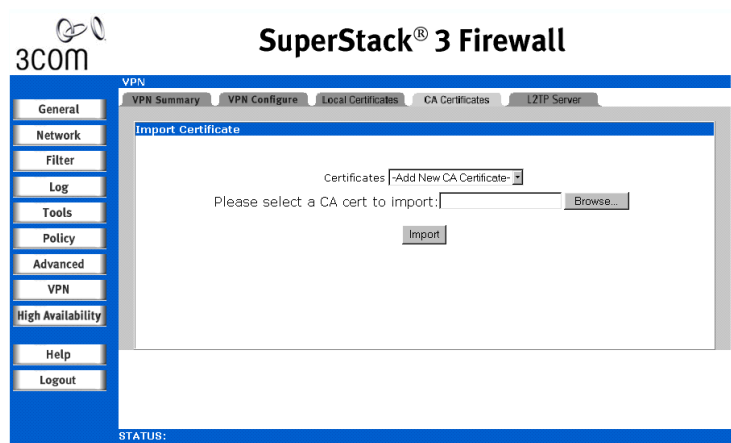
To implement the use of certificates for VPN SAs, you must obtain a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the Firewall to validate your local certificates.

Configuring the Firewall for use with CA Certificates

Once you have a validated CA Certificate you can import it into the Firewall and use it to validate Local Certificates for VPN Security Associations.

To configure the CA Certificates click on *VPN* and then select the *CA Certificates* tab. A window similar to that in [Figure 67](#) displays.

Figure 67 VPN CA Certificates Window



Import Certificate To import the CA Certificate, carry out the following:

- 1 Click *VPN* then *CA Certificates*.
- 2 Click *Browse* and locate the PKCS#7 encoded file sent by your CA service.
- 3 Click *Open* to set the directory path to the certificate and then click *Import* to upload the certificate into the Firewall. Once the certificate is imported, you can view the certificate details.



As certificates are time-stamped, ensure the Firewall has the correct date and time before importing them.

Viewing Certificate Details

The *Certificate Details* section shows the following information:

- Certificate Authority
- Subject Distinguished Name
- Certificate Issuer
- Certificate Serial Number
- Expiration Date

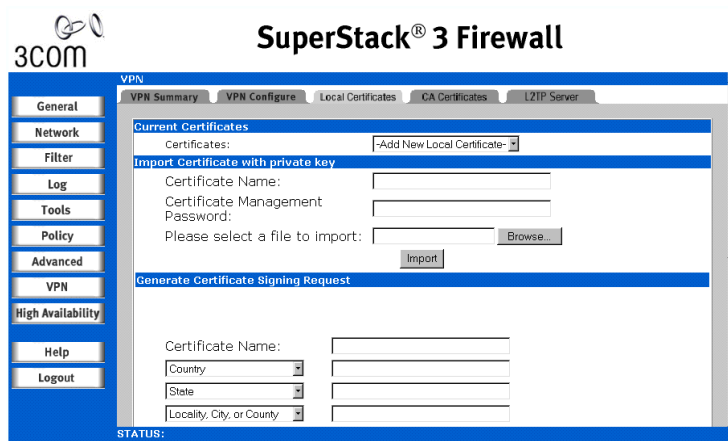
The *Certificate Issuer*, *Certificate Serial Number* and the *Expiration Date* are generated by the CA service. The information is used when a Generate Certificate Signing Request is created and sent to your CA service for validation.

To delete the certificate, click *Delete This Certificate*. You can delete a certificate if it has expired or if you decide not to use Third Party Certificates for VPN authentication.

Configuring the Firewall for use with Local Certificates

You will need to obtain a CA certificate first and import it into the Firewall to validate your local certificates. See [“Configuring the Firewall for use with CA Certificates”](#) on [page 170](#) for more information.

To configure the Local Certificates, click *VPN* and then select the *Local Certificates* tab. A window similar to that in [Figure 68](#) displays.

Figure 68 VPN Local Certificates Window**Current Certificates**

Both *Certificate Requests* and *Validated Certificates* appear in the list of *Current Certificates*. The *Certificate Details* section lists the same information as the *CA Certificate Details* section but a *Status* entry appears in the details. The status can be:

- *Request Generated* — Shows that the certificate has not been signed by the CA service.
- *Signed Certificate* — Shows the certificate is signed and ready for use.

Certificate Revocation List

A Certificate Revocation List (CRL) is a way to check the validity of an existing certificate. A certificate may be invalid for several reasons:

- It is no longer needed.
- A certificate was stolen or compromised.
- A new certificate has been issued that takes precedence over the old certificate.

If a certificate is invalid, the CA may publish the certificate on a CRL at a given interval, or on an online server in an X.509 v3 database using Online Certificate Status Protocol (OCSP). Consult your CA service for specific details on locating a CRL file or URL.



The Firewall supports obtaining the CRL through HTTP only.

You can import the CRL by locating the URL and importing it into the Firewall. Certificates are checked against the CRL by the Firewall for validity when they are used. You can also enter a URL location of the CRL by entering the address in the *Enter CRL's location for the CA (URL)* field. The CRL is downloaded at intervals determined by the CA service.

Import Certificate with Private Key

After a certificate is signed and returned by the CA service, you can import the certificate into the Firewall to be used as a Local Certificate for a VPN Security Association.

- 1 Click *VPN* then *Local Certificates*.
- 2 In the *Import Certificate with private key* section, enter the *Certificate Name*.
- 3 Enter the *Certificate Management Password*. This password was created when you exported your signed certificate.
- 4 Use *Browse* to locate the certificate file.
- 5 Click *Import* and the certificate appears in the list of *Current Certificates*.
- 6 To view details about the certificate, select it from the list of *Current Certificates*.



As certificates are time-stamped, ensure the Firewall has the correct date and time before importing them.

Generate Certificate Signing Request

To create a certificate for use with a VPN SA, carry out the following:



You must create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

- 1 Click *VPN* then *Local Certificates*.
- 2 In the *Generate Certificate Signing Request* section, enter a *Certificate Name*. Use the drop-down menus to enter information for the certificate request. As you enter information in the Request fields, the Distinguished Name (DN) is created. You may also attach an optional *Subject Alternative Name* such as the *Domain Name* or *E-mail Address*.
- 3 The *Subject Key* is preset as an RSA algorithm. RSA is a public key cryptographic algorithm used for encrypting data.
- 4 Select a *Subject Key Size*.

Not all key sizes are supported by a Certificate Authority. Check with your Certificate Authority for supported key sizes.

- 5 Click *Generate* to create a certificate file.

Once the certificate Signing Request is generated, a message describing the result is displayed.

- 6 Click *Export* to download the file to your computer and then click *Save* to save it to a directory on your computer.
- 7 When you have generated the Certificate Request, you can send it to your CA service for validation.

Importing a Signed Local Certificate

When the CA Service returns the signed certificate that you generated locally, import it into the Firewall as follows:

- 1 Click *VPN* then *Local Certificates*.
- 2 In the *Current Certificates* section, select the corresponding request from the *Certificates* menu.
- 3 Click *Browse* and select the *.der from the *Choose File* dialog box.
- 4 Click *Import Certificate*.

The Certificate is updated to *Verified* and you can now use it for creating a VPN SA using a third party certificate.



As certificates are time-stamped, ensure the Firewall has the correct date and time before importing them.

If you want to delete the certificate, click *Delete This Certificate*. You can delete a certificate if it has expired or if you decide not to use Third Party Certificates for VPN authentication. Click *Export This CA Certificate* to export the file to your hard drive or a floppy disk.

Configuring a VPN Security Association using IKE and a Third Party Certificate

To create a VPN Security Association using IKE and third party certificates, carry out the following:

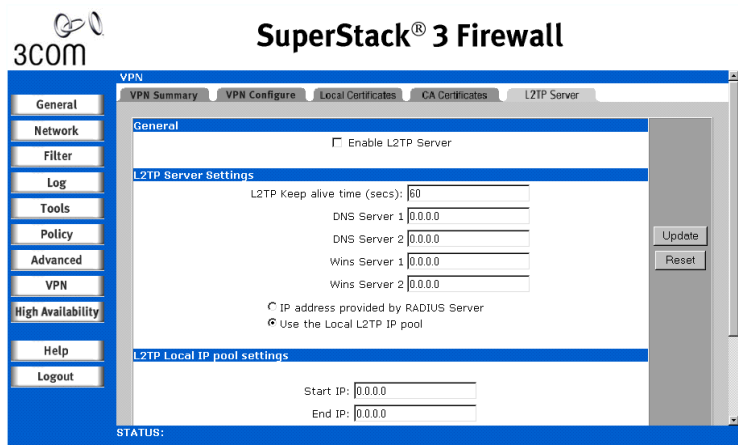
- 1 Click *VPN* and then *Configure*.
- 2 In the *Add/Modify IPSec Associations* section, select *IKE using 3rd party Certificates* from the *IPSec Keying Mode* menu.
- 3 Enter a *Name* for the Security Association.
- 4 Select a certificate from the *Select Certificate* list.
- 5 Enter the gateway address in the *IPSec Gateway Address* field.
- 6 In the *Security Policy* section, select the type of DH group from the *Phase 1 DH Group* menu.
- 7 The *SA Lifetime (secs)* automatically defaults 28800 seconds (8 hours).
- 8 Select the type of *Phase 1 Encryption/Authentication* from the menu.
- 9 Select the type of *Phase 2 Encryption/Authentication* from the menu.
- 10 In the *Peer Certificate's ID* section, you must select the *ID Type*. You can select *Distinguished Name*, *E-mail ID* or *Domain Name* from the menu. Then cut and paste the information from the Local Certificate into the text field.
- 11 In the *Destination Networks* section, select the type of destination for the VPN tunnel. *Use this SA as default route for all Internet traffic* can be used with only one SA. If you are allowing computers at the VPN destination to obtain an IP address dynamically through the tunnel, select *Destination network obtains IP addresses using DHCP through this SA*. If the VPN destination is a specific address, select *Specify destination network below* and click *Add new Network*. Enter the *Network IP Address* and *Subnet Mask* and click *OK*.

Configuring the Firewall as an L2TP Server

This section allows you to configure the Firewall as an L2TP server for use with L2TP VPN clients.

Click on *VPN* and then select the *L2TP* tab. A window similar to that in [Figure 69](#) displays.

Figure 69 VPN L2TP Window



General Click the *Enable L2TP Server* box if you want to run an L2TP server to authenticate L2TP VPN clients.

L2TP Settings L2TP Keep alive time (secs)

Enter the keep alive time for the L2TP connections. The default is 60 seconds.

DNS Server 1

A Domain Name Service (DNS) Server translates human readable host names into the numeric IP addresses used by computers to route information to the correct machine. You can use up to two DNS servers to improve performance and reliability. Enter the IP address of the first DNS Server.

DNS Server 2

Enter the IP address of an optional second DNS server.

WINS Server 1

A Windows Internet Name Service (WINS) Server provides a similar function as a DNS server but for Microsoft networks. Enter the IP address of the first WINS Server.

WINS Server 2

Enter the IP address of an optional second WINS server.

IP Address Provided by RADIUS Server

If you have enabled the RADIUS server to provide the IP address, check this button. Check also that you have enabled L2TP access for RADIUS users. See [“Configuring RADIUS User Privileges”](#) on [page 129](#) for more information.

Use the Local L2TP IP pool

If you want to use a local address pool, check this button and configure the IP address pool as described below.

**L2TP Local IP Pool
Settings**

If you are using the local L2TP pool to provide IP addresses for client connections, enter a range of IP addresses that can be used in the *Start IP* and *End IP* fields. The addresses must be on the same subnet as the LAN and you must take care to allocate addresses not in use by other clients or servers or already issued by the DHCP server.

L2TP Active Sessions

This section displays the details and status of any L2TP sessions.

10

CONFIGURING HIGH AVAILABILITY

This chapter describes the commands and options available in the *High Availability* menu. The menu is broken up into sections shown in the user interface as tabs.

To access a command click *High Availability* and then the appropriate tab.

The following sections are covered in this chapter:

- [Getting Started](#)
- [Configuring High Availability](#)
- [Checking High Availability Status](#)
- [Forcing Transitions](#)

Getting Started

The High Availability function allows you to connect two Firewalls together as a pair. Although only one Firewall will function at a time the second automatically takes over from the first in the event of a failure.

Before attempting to configure two Firewalls as a High Availability pair, check the following requirements:

- You have two Superstack 3 Firewalls available. The Firewalls must be running the same version of firmware which must be version 6.3 or above. This version of firmware is required to ensure the Synchronize function described in this chapter can work.



The 3Com Firewalls 3CR16110-95 and 3CR16110-97 use identical hardware and can be used as a high availability pair provided that they are using the same version of firmware.

- You have at least one static IP address available from your Internet Service Provider (ISP). If you intend to remotely manage both the primary Firewall and the backup Firewall then two addresses are required.



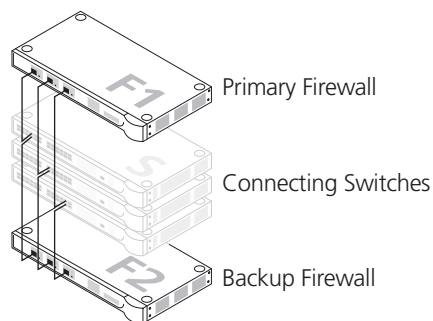
High Availability does not allow the use of dynamic IP address assignment from your ISP.

- Each Firewall in the High Availability pair must have the same upgrades and subscriptions enabled. If the backup unit does not have the same upgrades and subscriptions enabled, these functions are not supported in the event of a failure of the primary Firewall.

Network Configuration for High Availability Pair

The following diagram illustrates the network configuration for a High Availability pair:

Figure 70 Two Firewalls connected as a High Availability Pair



CAUTION: Do not mix the LAN, DMZ and WAN networks when connecting the Firewalls together as this will compromise the security of your network.

All Firewall ports being used must be connected together with a hub or switch. Each Firewall must have a unique LAN IP Address on the same LAN subnet. If each Firewall has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.



The two Firewalls in the High Availability pair send “heartbeats” over the LAN network segment. The High Availability feature does not function if the LAN ports are not connected together.

Configuring High Availability

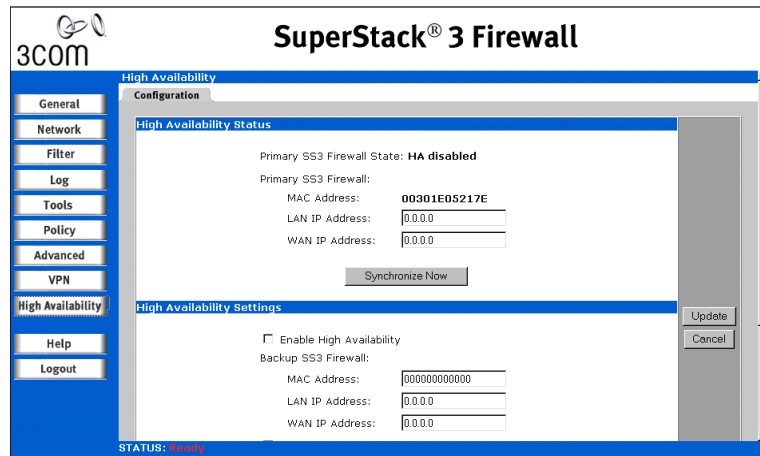
Configuring a High Availability pair of Firewalls consists of two steps:

- [Configuring High Availability on the Primary Firewall](#)
- [Configuring High Availability on the Backup Firewall](#)

Both steps must be completed before the two Firewalls can function as a High Availability pair.

Click *High Availability* and then click *Configure*. A window similar to the one in [Figure 71](#) displays.

Figure 71 High Availability Menu



Viewing the High Availability Status

The top half of the window displays the primary Firewall's serial number and network settings. The bottom half of the window is used to configure High Availability:

MAC Address

The serial number of the primary Firewall is displayed. This field is read-only.

LAN IP Address

Enter the *LAN IP Address* of the primary Firewall that the primary Firewall will transition to if an active Firewall is detected on the network. This setting is optional and is only required to allow administrative access to the Management Interface when the Firewall is in idle mode

WAN IP Address

Enter the *WAN IP Address* of the primary Firewall. This is an optional setting and is only required to allow remote access to the Management Interface when the Firewall is in idle mode. If this setting is configured, it must be a unique IP address on the same WAN subnet as the *Firewall WAN IP Address* in the *Network* window.

Synchronize Now

Click this button to force an upload of the configuration of the primary Firewall to the backup Firewall. The backup Firewall restarts and automatically synchronizes with the primary Firewall after the restart. See [“Configuring High Availability on the Backup Firewall”](#) below for more information.



Clicking Synchronize Now restarts the backup Firewall.

Configuring High Availability on the Primary Firewall

To configure High Availability on the Primary Firewall carry out the following:

- 1 To enable *High Availability*, check the *Enable High Availability* box.
- 2 Enter the *MAC Address*, *LAN IP Address* and *WAN IP Address* of the backup Firewall.



The MAC Address and LAN IP Address are required settings for the backup Firewall. The WAN IP Address field may be left blank if remote management is not required for the backup Firewall.

- 3 Check the *Preempt mode* check box to cause the primary Firewall to take over from the backup Firewall whenever the primary is available (for example, after recovering from a failure and restarting).



The primary and backup Firewalls use a “heartbeat” signal to communicate with one another. This heartbeat is sent between the Firewalls over the network segment connected to the LAN ports of the two Firewalls. The interruption of this heartbeat signal triggers the backup Firewall to take over operation from the active unit of the High Availability pair. The time required for the backup Firewall to take over from the active unit depends on the Heartbeat Interval and the Failover Trigger Level.

- 4 Enter the *Heartbeat Interval* time in seconds. This interval is the amount of time in seconds that elapses between heartbeats passed between the two Firewalls in the High Availability pair.
- 5 Enter the *Failover Trigger Level* in terms of the number of missed heartbeats. When the backup unit detects this number of consecutive missed heartbeats, the backup Firewall takes over operation from the active unit.

If, for example, the *Heartbeat Interval* and the *Failover Trigger Level* are 5 seconds and 2 missed heartbeats respectively, the backup Firewall takes over from the primary Firewall after 10 seconds in the event of a failure in the primary Firewall.

- 6 Click *Update*. Once the Firewall has been updated, a message confirming the update is displayed at the bottom of the browser window. If you have modified the *Enable High Availability* setting, you must restart the Firewall for change to take effect.

Configuring High Availability on the Backup Firewall

The backup Firewall should not be configured through the Web interface. Instead, once you have configured the Primary Firewall and connected the two units together as shown in [Figure 70](#) on [page 180](#). Power on the backup Firewall. The backup Firewall is automatically detected by the primary Firewall and the settings are automatically synchronized between the two firewalls.

The configuration of the primary Firewall is uploaded to the backup Firewall. This method assures uniform configuration of the two Firewalls in the High Availability pair. Future changes to the primary Firewall's configuration are automatically uploaded to the backup Firewall.

Firmware Upgrades

Firmware upgrades must be performed separately for the primary and backup Firewalls. See ["Upgrading the Firewall Firmware"](#) on [page 109](#) for instructions on upgrading firmware.

Checking High Availability Status

If a failure of the primary Firewall occurs, the backup Firewall assumes the primary Firewall's LAN and WAN IP Addresses. It is therefore not possible to determine which Firewall is active by logging into the LAN IP Address alone.

There are three ways you can check the status of the High Availability pair:

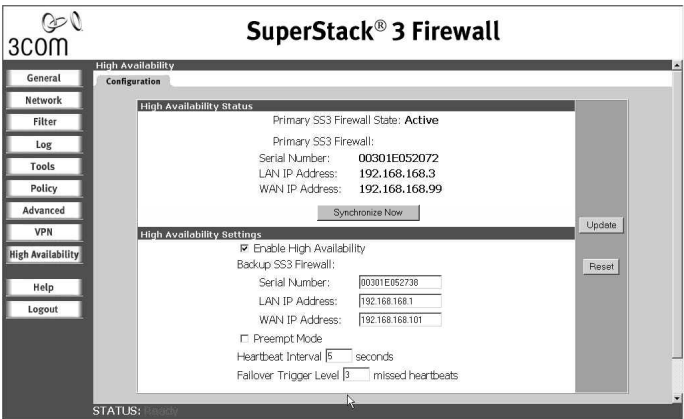
- Check the High Availability Status Window
- Watch for E-mail Alerts.
- View the Log.

These methods are described below.

**High Availability
Status Window**

One method to determine which Firewall is active is to check the High Availability status page for the High Availability pair. To view the High Availability status window, open primary Firewall's LAN Web interface. Click *High Availability* and then click *Configuration*. If the primary Firewall is active, a window similar to the following is displayed.

Figure 72 High Availability Status Window



The first line in the status window above indicates that the primary Firewall is currently Active.

If the backup Firewall has taken over for the primary, for example, in the event of a failure to the primary Firewall, the first line in the status window indicates that the backup Firewall is currently Active.

Check the status of the backup Firewall by logging into the LAN IP Address of the backup Firewall. If the primary Firewall is operating normally, the status window indicates that the backup Firewall is currently Idle. If the backup has taken over for the primary, this window indicates that the backup is currently Active.



In the event of a failure in the primary Firewall, you may access the Web interface of the backup Firewall at the primary Firewall's LAN IP Address or at the backup Firewall's LAN IP Address.

E-Mail Alerts Indicating Status Change

If you have configured the primary Firewall to send e-mail alerts, you will receive an alert e-mail when there is a change in the status of the High Availability pair. For example, when the backup Firewall takes over from the primary after a failure, an e-mail alert is sent indicating that the backup has transitioned from Idle to Active. If the primary Firewall subsequently resumes operation after that failure, and *Preempt Mode* has been enabled, the primary Firewall takes over and another E-mail alert is sent to the administrator indicating that the primary has preempted the backup.

View Log

The Firewall also maintains an event log that displays these High Availability events in addition to other status messages and possible security threats. This log may be viewed with a browser using the Firewall Web interface or it may be automatically sent to the administrator's e-mail address. To view the Firewall log, click *Log* and then click *View Log*. A window similar to the following is displayed.

Figure 73 Log Screen Showing Switchover of Firewall

Time	Message	Source	Destination	Notes	Rule
23/07/2001 07:46:03.336	SuperStack 3 activated				
23/07/2001 07:46:08.144	ARP timeout	0.0.0.0	192.168.168.100		
23/07/2001 07:46:08.240	Primary firewall has transitioned to Idle				
23/07/2001 07:46:24.000	Primary missed heartbeats from Active Backup: Primary going Active				
23/07/2001 07:46:24.000	Primary firewall has transitioned to Active				
23/07/2001 07:46:31.912	Broadcast packet dropped	192.168.168.2, 520, LAN	255.255.255.255, 520, LAN	Code:17	
23/07/2001 07:46:33.480	Firewall access from LAN	192.168.168.4, 1660, LAN	192.168.168.3, 80, LAN		
23/07/2001 07:46:46.144	Successful administrator login	192.168.168.4, LAN	192.168.168.3		
23/07/2001 07:47:39.544	Firewall access from LAN	192.168.168.4, 1715, LAN	192.168.168.3, 80, LAN		

Forcing Transitions

In some cases, it may be necessary to force a transition from one active Firewall to another – for example, to force the primary Firewall to become active again after a failure when *Preempt Mode* has not been enabled, or to force the backup Firewall to become active in order to do preventative maintenance on the primary Firewall.

To force such a transition, it is necessary to interrupt the heartbeat from the currently active Firewall. This may be accomplished by disconnecting the active Firewall's LAN port, by shutting off power on the currently active unit, or by restarting it from the Web interface. In all of these cases, heartbeats from the active Firewall are interrupted, which forces the currently Idle unit to become Active.

To restart the active Firewall:

- 1 Open the primary Firewall's Web interface.
- 2 Click *Tools*.
- 3 Click *Restart*.
- 4 Click *Restart SuperStack 3 Firewall*, then *Yes* to confirm the restart.

Once the active Firewall restarts, the other Firewall in the High Availability pair takes over operation.



CAUTION: *If the Preempt Mode box has been checked for the primary Firewall, the primary unit takes over operation from the backup unit after the restart is complete.*



ADMINISTRATION AND TROUBLESHOOTING

[Chapter 11](#) Administration and Advanced Operations

[Chapter 12](#) Troubleshooting



11

ADMINISTRATION AND ADVANCED OPERATIONS

This chapter provides some background on Firewall concepts and describes some administration functions not available through the menu structure. The following sections are covered in this chapter:

- [Introducing the Web Site Filter](#)
- [Activating the Web Site Filter](#)
- [Using Network Access Policy Rules](#)
- [Resetting the Firewall](#)
- [Direct Cable Connection](#)

Introducing the Web Site Filter

The 3Com SuperStack® 3 Web Site Filter (3C16111) provides the SuperStack 3 Firewall with enhanced Internet filtering capabilities. It can control access from the LAN to thousands of Web sites that might be deemed inappropriate for business use. Twelve selectable Web site categories are provided so Internet access can be tailored to the needs of the organization. Just like the Custom List and filtering by Keywords (see [Chapter 5](#)), access to these sites can be enabled or disabled.

The 3Com Web Site Filter is provided as a 12-month subscription, and can be automatically updated weekly to ensure that the filter keeps pace with the ever-changing Internet.

The Firewall comes with a one-month subscription free of charge.

The 3Com Web Site Filter uses the CyberNOT list, which is licensed from The Learning Company. This list is developed and maintained by The Learning Company's Cyber Patrol unit.

The sites on the CyberNOT List are reviewed by a team of Internet professionals, including parents and teachers. They use a set of criteria

that categorizes Internet sites and resources according to the level of possibly objectionable content.

In evaluating a site for inclusion in the list, the team consider the effect of the site on a typical twelve year old searching the Internet unaccompanied by a parent or educator. Any easily accessible pages with graphics, text or audio which fall within the definition of the categories below is considered sufficient to place the source in the category.

- Violence/Profanity:

Violence: pictures exposing, text or audio describing extreme cruelty, physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Profanity: is defined as obscene words or phrases either audio, text or pictures.

- Partial Nudity:

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia. The Partial Nudity category does not include swimsuits (including thongs).

- Full Nudity:

Pictures exposing any or all portions of the human genitalia. Please note: The Partial Nudity and Full Nudity categories do not include sites containing nudity or partial nudity of a non-prurient nature. For example: web sites for publications such as National Geographic or Smithsonian Magazine or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

- Sexual Acts:

Pictures, descriptive text or audio of anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior, including masturbation, copulation, pedophilia, intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, adult personal ads, CD-ROMs and videos.

- Gross Depictions:

Pictures, descriptive text or audio of anyone or anything which are crudely vulgar or grossly deficient in civility or which show scatological impropriety. Includes such depictions as maiming, bloody figures, autopsy photos or indecent depiction of bodily functions.

- Intolerance:

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

- **Satanic/Cult:**

Satanic material is defined as: Pictures or text advocating devil worship, an affinity for evil, or wickedness. A cult is defined as: A closed society, often headed by a single individual, where loyalty is demanded, leaving may be punishable, and in some instances, harm to self or others is advocated.

Common elements may include: encouragement to join, recruiting promises, and influences that tend to compromise the personal exercise of free will and critical thinking.

- **Drugs/Drug Culture:**

Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This category does not include material about the use of illegal drugs when they are legally prescribed for medicinal purposes (e.g., drugs used to treat glaucoma or cancer).

- **Militant/Extremist:**

Pictures or text advocating extremely aggressive and combative behavior, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes: How to, information on weapons making, ammunition making or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.

- **Sex Education:**

Pictures or text advocating the proper use of contraceptives. This topic would include condom use, the correct way to wear a condom and how to put a condom in place. Also included are sites relating to discussion about the use of the Pill, IUDs and other types of contraceptives. In addition to the above, this category will include discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries. The Sex Education category is uniquely assigned; sites classified as Sex Education are not classified in any other category. This permits the user to block or allow the Sex Education category as appropriate, for example, allow the material for an older child while restricting it for a younger child.

Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Sex Acts category.

- **Questionable/Illegal & Gambling:**

Pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission) and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting, including non-monetary dares and "1-900" type numbers.

- **Alcohol & Tobacco:**

Pictures or text advocating the sale, consumption, or production of alcoholic beverages or tobacco products, including commercial sites in which alcohol or tobacco products are the primary focus. Pub and restaurant sites featuring social or culinary emphasis, where alcohol consumption is incidental are not in this category

For further details refer to:

<http://www.cyberpatrol.com>

Activating the Web Site Filter

When you register the Firewall you are given 30 days free subscription to the Web Site Filter. To continue getting upgrades to the Web Site Filter (covering new Web Sites as they appear) you need to purchase the annual Web Site Filter subscription.

To activate your annual subscription perform the following steps:

- 1 Using a Web browser, go to the Firewall registration page
<http://www.3com.com/ssfirewall/>
- 2 Click the *Web Site Filter Registration* link.
- 3 In the box labeled *Serial Number*, type the Internet Firewall's serial number



The Firewall's serial number is printed on the bottom of the Firewall and is also displayed at the top of the Status window in the Web interface.

- 4 In the *Activation Key* box, type the key supplied with the Web Site Filter.
- 5 Click *Activate*.

After a short while, a message confirming the subscription's activation is displayed in the Web browser window.



You must have already registered the Firewall before Activating the Web Site Filter.

Using Network Access Policy Rules

Network Access Policy Rules are the tools you use to control traffic between the LAN, DMZ and WAN ports of your Firewall.

Use this list to help you create rules.

- State the intent of the rule.

The following are examples of intent for rules:

- This rule will restrict all IRC access from the LAN to the Internet.
- This rule will allow a remote Lotus Notes server to synchronize over the Internet to an internal Notes server.
- Is the intent of the rule to allow or deny traffic?
- What is the flow of the traffic: from the LAN to the Internet, or from the Internet to the LAN?
- List which IP services will be affected.
- List which computers on the LAN will be affected.
- List which computers on the Internet will be affected.

The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

Once you have defined the logic of the rule, it is critical to consider the security ramifications created by the rule:

- Will this rule stop LAN users from accessing critical resources on the Internet?

For example, if IRC is blocked, are there users that require this service?

- Is it possible to modify the rule to be more specific?

For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

- Will this rule allow Internet users access to resources on the LAN in a manner that may create an undue security vulnerability?

For example, if NetBIOS ports (UDP 137, 138, 139) are allowed from the Internet to the LAN, Internet users may be able to connect to PCs with file sharing enabled.

- Does this rule conflict with any existing rules?

Once you have answered these questions, to add rules you type the information into the correct boxes in the *Policy Rules* window.

a *Action*

Click *Allow* or *Deny* depending on the intent of the rule, as defined by item 2 in the [“Using Network Access Policy Rules”](#) on [page 193](#).

b *Service*

From the *Service* menu, select the IP protocol, as defined by item 4 in the [“Using Network Access Policy Rules”](#) on [page 193](#). If the protocol is not listed, it is necessary to first define it in the *Add Service* window.

c *Source*

There are three parameters to configure for the *Source* item.

- Select the Network Access Rule’s source port, *LAN*, *WAN*, or *DMZ*, if appropriate, from the *Ethernet* menu.
- If there are IP address restrictions on the source of the traffic, such as keeping competitors off the company’s Web site, type the starting and ending IP addresses of the range in the *Addr. Range Begin* and *Addr. Range End*, respectively.
- If all IP addresses are affected, type * in the *Addr. Range Begin* box.

d *Destination*

There are three parameters to configure for the *Destination* item.

- Select the Network Access Rule’s destination port, *LAN*, *WAN*, or *DMZ*, if appropriate, from the *Ethernet* menu.
- If there are IP address restrictions on the destination of the traffic, such as limiting Telnet to a remote site, type the starting and ending IP addresses of the range in the *Addr. Range Begin* and *Addr. Range End*, respectively.
- If all IP addresses are affected, type * in the *Addr. Range Begin* box.

Understanding the Rule Hierarchy

The rule hierarchy has two basic concepts:

- Specific rules override general rules.
- Equally specific Deny rules override Allow rules.

When evaluating rules, the Firewall uses the following criteria:

- A rule defining a specific service is more specific than the default rule.
- A defined Ethernet link, such as LAN, WAN, or DMZ, is more specific than * (all).
- A single IP address is more specific than an IP address range.

Rules are listed in the Web interface from most specific to the least specific, and rules at the top override rules listed below.

Examples of Network Access Policies

The following examples illustrate methods for creating Network Access Policy Rules.

Blocking LAN Access to Specific Protocols

This example shows how to block all LAN access to NNTP servers on the Internet.

- 1 For the Action, choose *Deny*.
- 2 From the *Service* list, choose *NNTP*.
If the service is not listed in the menu, add it in the *Add Service* window.
- 3 Select *LAN* from the *Source Ethernet* list.
- 4 Since all computers on the LAN are to be affected, enter * in the *Source Addr. Range Begin* box.
- 5 Select *LAN* from the *Destination Ethernet* menu.
- 6 Since the intent is to block access to all NNTP servers, enter * in the *Destination Addr. Range Begin* box.
- 7 Click *Add Rule*.

Block Access to Specific Users

This example shows how to create a rule which blocks a certain range of computers, such as a competitor, from accessing the public Web server on the LAN or DMZ.

- 1 For the Action, choose *Deny*.
- 2 From the *Service* list, choose *HTTP*.
- 3 Select *WAN* from the *Source Ethernet* list.

- 4 Enter the blocked network's starting IP address in the *Source Addr. Range Begin* box and the blocked network's ending IP address in the *Source Addr. Range End* box.
- 5 Select *** from the *Destination Ethernet* list.
- 6 Since the intent is to block access to all servers, enter *** in the *Destination Addr. Range Begin* box.
- 7 Click *Add Rule*.

Enabling the ISP to Ping the Firewall

By default, the Firewall does not respond to pings from the Internet. However, Ping is a tool that many ISPs use to verify that the Internet connection is active.

In this example, you limit the source to allow the ISP to ping the Firewall only.

- 1 For the Action, choose *Allow*.
- 2 From the *Service* list, choose *Ping*.
- 3 Select *WAN* from the *Source Ethernet* list.
- 4 Enter the starting IP address of the ISP's network in the *Source Addr. Range Begin* box and the network's ending IP address in the *Source Addr. Range End* box.
- 5 Select *LAN* from the *Destination Ethernet* list.
- 6 Since the intent is to allow a ping only to the Firewall, enter the Firewall's LAN IP Address in the *Destination Addr. Range Begin* box.
- 7 Click *Add Rule*.

Restore the Default Network Access Rules

If the Firewall's network access rules have been modified or deleted, the administrator may wish to restore them to the factory default settings. The default rules block all incoming traffic from the WAN to the LAN and allow all outgoing traffic from the LAN to the WAN.

Click *Restore Rules to Defaults* at the bottom of the Rules page to restore the default network access rules. A dialog box displays the message, *This will erase all settings you have made on the Services and Rules tab*. Click *OK* and restart the Firewall for the changes to take effect.



Restoring the default rules deletes all custom rules and Public LAN Servers. If an IKE VPN Security Association has been created, a service will need to be recreated to permit IKE negotiations.

Protocols/Services to Filter

Although the Firewall is shipped in a safe mode by default, the user can alter the Policy Rules and potentially cause the Firewall to be vulnerable to attacks. Therefore, before any modifications are made, the user should be aware of which services are of most risk to the private LAN.

The following table shows the protocols that are inherently vulnerable to abuse and should be blocked from entering or leaving the site.

Table 8 Protocol Definitions and Characteristics

Protocol Name	Port Number	Risk
TFTP-Trivial FTP	69	This protocol can be used to boot diskless workstations, terminal servers and routers, and can also be used to read any file on the system, if set up incorrectly.
X Windows	6000+	This can leak information from X window displays including all keystrokes.
DNS-Domain Names Service	53	The DNS service contains names of hosts and information about hosts that could be helpful to attackers.
RIP-Routing Information Protocol	520	This service can be used to redirect packet routing.
UUCP-UNIX-to-UNIX CoPy	540	If this service is not properly configured, it can be used for unauthorized access.
Open Windows	2000	This protocol can also leak information about what keystrokes are depressed.
RPC-Remote Call Procedure	111	The RPC services, including NIS and NFS, can be used to steal system information such as passwords and read to write files.
Rexec	512	These protocols can permit unauthorized access to accounts and commands
Rlogin	513	
Rsh	514	
Other services, whether inherently dangerous or not, should be restricted to only those systems that need them as shown below:		

Table 8 Protocol Definitions and Characteristics

Protocol Name	Port Number	Risk
Telnet	23	Restrict to certain systems
FTP-File Transfer Protocol	20,21	Restrict to certain systems
SMTP-Simple Mail Transfer Protocol	25	Restrict to central e-mail server

While some of these services such as TELNET or FTP are inherently risky, blocking access to these services completely may be too drastic a policy for many sites. Not all systems, though, generally require access to all services. For example, restricting TELNET or FTP access from the Internet to only those systems that require the access can improve security at no cost to user convenience.

Services such as NNTP (Network News Transfer Protocol) may seem to pose little threat, but restricting these services to only those systems that need them helps to create a cleaner network environment and reduces the likelihood of exploitation from yet-to-be-discovered vulnerabilities and threats.

Resetting the Firewall

You cannot retrieve a lost administrator password from the Firewall. If you want to reset your Firewall to factory default settings, and can access the Web interface of the Firewall successfully, 3Com recommends that you use the [“Restoring Factory Default Settings”](#) command, described on [page 108](#).

However, if it is no longer possible to access the Web interface (for example, due to a lost password), then you must completely reset your Firewall.



CAUTION: *The reset procedure described below not only deletes all the settings from your Firewall, but also erases the current copy of the firmware from the unit. For this reason, 3Com recommends that you save your Firewall settings on a regular basis, and that you also have a copy of the latest firmware available locally. A copy is available on the companion CD to get you up and running again.*

Resetting the Firewall To reset the Firewall:

- 1 Disconnect the power from the Firewall.
- 2 Using a blunt pointed object, fully press in the reset button on the back panel.
- 3 Whilst holding this button in, reconnect the power to the unit.
- 4 Continue holding the reset button in until the Alert LED starts flashing. This should be approximately 20 seconds.
- 5 When the Alert LED stops flashing, the reset is complete. You can now release the reset button.

When the reset is complete, the Firewall restarts. The Power LED stops flashing and the Alert LED is illuminated continuously, indicating that the unit has been reset and the firmware erased.

Reloading the Firmware

Even when the firmware has been erased, you can use a basic Web interface to get the Firewall up and running again. The Firewall reverts to its default IP address of **192.168.1.254** after a complete reset, so you must reconfigure your chosen management station to an IP address in the same subnet to access the Web interface.

To reload the firmware:

- 1 Type **http://192.168.1.254** into the web browser on the management station, and press *Enter*. The basic Web interface loads, similar to that shown in [Figure 74](#).

Figure 74 Firmware Upload Window

The current firmware file appears to be corrupted.

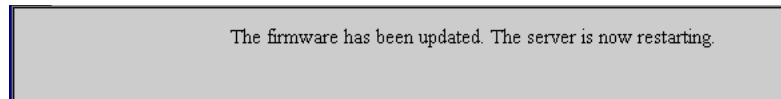
Please select a firmware file:

- Use the browse button to find the firmware file you want uploaded into your box.
- Make sure not to interrupt the browser or close the browser window while the firmware is uploading.
- Refer to your product documentation for more information on recovering from corrupt firmware.
- After the firmware is uploaded, the box will automatically restart.

Make sure that you are using the browser that supports HTML uploads, otherwise you cannot upload the firmware.

- 2 In the box labeled *Please select a firmware file*, type in the full file and path name of the firmware image that you want to upload to the unit. Use the *Browse* button to locate the file if you are not sure of its location.
- 3 Once you have located the file, click *Upload* to upload the firmware. This process takes approximately one minute. Once complete, the Firewall restarts automatically, and the message shown in [Figure 75](#) is displayed.

Figure 75 Firmware Upload Complete



The self-test cycle should now complete successfully. If the entire process has been successful, the power LED should light up and remain on after 90 seconds, and the Alert LED should remain off. You can now access the firmware at the default IP address of 192.168.1.254. The default user name is `admin`, and the default password is `password`.

Once you have logged into the Web interface, you may upload your saved settings file, as described in [“Importing the Settings File”](#) on [page 107](#). Note that the administrator password is not uploaded, and is still `password` once the upload is complete. Make sure that you change this password to increase the security of the unit.

If you do not have a saved settings file, you must set up the unit from scratch using either the Installation Wizard described in [Chapter 3](#) or using the commands provided through the Web interface described in the rest of this guide.

Direct Cable Connection

The security of the Firewall is ensured by the use of a secret Administrator Password. Once the password is set, it is used to authenticate the administrator’s identity as well as to conceal any important information exchanged with the Web interface. For example, when the administrator’s password is changed, the old password is used to conceal the new one.

The Firewall comes pre-configured from the factory with a default password. It is critical to change this password during the initial

configuration of the Firewall. Unfortunately, the default password can only provide limited protection the first time the administrator's password is set. In principle, an individual inside the network could capture all network transmissions and then perform mathematical analyses to discover the new Administrator Password. Though this is more an academic than a practical issue, using the *Direct Connection* option to set the password for the first time may be advisable if this is a concern.

Direct Connection Instructions

To connect a management station directly to the Firewall complete the following:

- 1 Disconnect the management station from the local Ethernet network.
- 2 Attach the Firewall directly to the management station.
To do this, connect a cable from the Ethernet port on the management station to the LAN Port of the Firewall.
- 3 Switch on the Firewall.
To do this, connect the power adapter to the port on the back labeled Power.
- 4 Wait for the Power LED to stop flashing. This takes approximately 90 seconds.
- 5 Follow the initial configuration steps as described in [Chapter 3](#).
- 6 Disconnect the management station from the Firewall and reconnect it to the main Ethernet network.
In some cases, you may have to restart the management station after reconnecting it.
- 7 Attach the Firewall to the LAN (see [Chapter 3](#)) and continue with configuration.

12

TROUBLESHOOTING

This chapter contains the following:

- [Introduction](#)
- [Potential Problems and Solutions](#)
- [Troubleshooting the Firewall VPN Client](#)
- [Frequently Asked Questions about PPPoE](#)

Introduction

The Firewall has been designed to help you detect and solve possible problems with its installation and operation in your network. If you cannot find the solution to the problem in this chapter, please contact Technical Support (see [Appendix D](#) for information about contacting Technical Support).

First, try the following:

- Make sure that all equipment is switched on.
- Switch off the Firewall, wait approximately 5 seconds, and then switch it back on. Wait for the Power LED to stop flashing (approximately 90 seconds).



CAUTION: *The contents of the log are lost when resetting the Firewall. If you are trying to diagnose a repeating problem examine the log before resetting the Firewall.*

Potential Problems and Solutions

The following is a list of problems you may experience with your Firewall with some suggested solutions.

Power LED Not Lit

Check if the power cord is plugged into a live power socket.

Power LED Flashes Continuously	If the Power LED continues to flash after 120 seconds, please contact Technical Support (see Appendix D for information about contacting Technical Support).
Power and Alert LED Lit Continuously	If the Power and Alert LEDs are both continuously lit, please contact Technical Support (see Appendix D for information about contacting Technical Support).
Link LED is Off	<p>If the Link LED is not lit, try the following:</p> <ul style="list-style-type: none">■ Make sure the Firewall is powered on.■ Make sure the RJ-45 connections are secure. Gently moving the cable back and forth should not make the Link LED turn on and off.■ Make sure the wiring follows the CAT-5 specification. See “Pinout Diagrams” on page 245 for more information.■ Try replacing the cable with a known good cable.■ Try using a standard CAT-5 cable. If the problem is on the LAN or DMZ port, try setting the Uplink/Normal switch to the alternative position.
Ethernet Connection is Not Functioning	<p>If the Ethernet connection does not work, try the following:</p> <ul style="list-style-type: none">■ Check the physical connections to make sure they are secure.■ Try replacing the cable with a known good cable.
Cannot Access the Web interface	<p>If the Firewall does not allow users or the administrator to log in to establish an authenticated session, try the following:</p> <ul style="list-style-type: none">■ Make sure that the Web browser you are using to access the Web interface is supported by the Firewall. Netscape Navigator 4 or Internet Explorer 4 or higher versions are supported.■ During the initial configuration, make sure that you change the IP address for the management station to one in the same subnet as the Firewall, such as 192.168.1.200.■ Make sure the Web browser has Java, JavaScript, or ActiveX enabled.■ Make sure the users are attempting to log into the correct IP address. The correct address is the management IP Address of the Firewall, and not the Public Address, if NAT is enabled.■ Make sure that users are attempting to log in with a valid user name and password.

- Remember that passwords are case-sensitive; make sure the Caps Lock key is off.
- Click *Reload* or *Refresh* in the Web browser and try again. For security reasons, the Firewall sends a slightly different Authentication page each time you log in to the Web interface. If the password you use does not allow access to the Firewall, it might be because the browser is displaying a cached copy of the page instead of the current page.
- If you cannot remember the correct password, you can reset the Firewall. See [“Resetting the Firewall”](#) on [page 199](#) for more information.

LAN Users Cannot Access the Internet

If your users cannot access the Internet, try the following:

- If NAT is enabled, make sure the default router address on the LAN Client is set to the Management IP Address of the Firewall.
- If there are any host devices other than the Internet router connected to the WAN port, they are not accessible to users on the LAN.
- To see if the problem is outside the Firewall, disconnect the Firewall and try to access the Internet.
- Try restarting the router and LAN machines.
- If you are using the Internet Firewall with a cable modem, you may need to register the MAC address of the unit with your cable service provider before connecting the Internet Firewall to your network. You can find the MAC address of the Internet Firewall on a label on the underside of the unit.

Firewall Does Not Save Changes

If the Firewall does not save the changes that you make, make sure that you click *Update* before moving to another window or tab, or all changes are lost.

Duplicate IP Address Errors Are Occurring

If there are duplicate IP address errors after you have installed the Firewall:

- Try restarting the router or LAN machines.
- Make sure the LAN is not connected to the WAN port on the Firewall.
- If DHCP is on, make sure no other DHCP servers are on the LAN.

Machines on the WAN Are Not Reachable

Make sure the Intranet settings in the *Advanced* section are correct.

Troubleshooting the Firewall VPN Client

If the Firewall client is unable to negotiate with the Firewall, the Firewall VPN Client Viewer displays detailed error messages. To access the Log Viewer, select and right click on the icon in the Windows Task Bar and then select Log Viewer.

To view Log messages, try to initiate a VPN session, either by attempting to log into the remote Firewall Web interface, or by pinging a machine on the remote network.

The Log Viewer displays any VPN negotiation errors, such as invalid SPIs or invalid keys.

Error Message Explanations

- "New Connection - Initiating IKE Phase 1 (IP ADDR=10.0.030)

New Connection - SENDING...ISAKMP OAK AG
(SA, KE, NON, ID, VID)

New connection - message not received! Retransmitting!"

This means the VPN client cannot contact the Firewall either because the VPN client is misconfigured, or the Internet Service Provider for either the Firewall or the VPN client does not pass IPSec packets.

- IreIKE:Unable to acquire CAPI provider handle

This indicates that the Firewall VPN client did not install properly. Completely uninstall the VPN client, restart your computer, and then reinstall the VPN client to ensure the client software functions correctly. Confirm that any other IPSec VPN clients have been removed before reinstalling the Firewall VPN client.

The IKE Negotiation on the VPN Client

The IKE Negotiation on the VPN Client requires a certain amount of processor time, before the tunnel opens. This usually takes a few seconds to complete and some packets may be lost during the process.



There is no negotiation time when using Manual Keys

Restarting the Firewall with Active VPN Tunnel

If you restart the Firewall with a VPN Client active you must deactivate and reactivate the IRE VPN Client. Restarting the Firewall kills all the current VPN tunnels on the Firewall side. In this case the IRE VPN assumes that the connection is still intact and sends encrypted packets that eventually get dropped.

A easy way to restart the negotiation on the client side is to click on the floppy disk icon at the top of the Security Policy Editor screen.

Export the VPN Client Security Policy File

- 1 Select *Export Security Policy* in the *File* menu at the top of the *Security Policy Editor* window.
- 2 Click *Yes* to lock the Security Policy and prevent remote users from changing the VPN client policy. Click *No* to permit remote user configuration. Then name the security policy database file (*.spd) and save it to a local folder or to a floppy disk.

Import the VPN Client Security Policy File

- 1 Select *Import Security Policy* in the *File* menu at the top of the *Security Policy Editor* window.
- 2 Browse your local hard drive for the desired security policy database file (*.spd) and click *Open*.

Uninstall the VPN Client

- 1 To uninstall the Firewall VPN Client, open the *Control Panel* in the Windows *Start* menu.
- 2 Double click *Add/Remove Programs* in the Control Panel window.
- 3 Select *IRE VPN Client* in the Add/Remove Programs Properties window and click *Add/Remove*.
- 4 Click *Yes* in the Confirm File Deletion window to delete the VPN client and all of its components.
- 5 Click *Yes* to save the security policy database file to the Firewall VPN Client.

Frequently Asked Questions about PPPoE***Why are ISPs using PPPoE in their broadband services?***

The theory is that PPPoE makes it easier for the end user of broadband services to connect to the Internet by simulating a Dial-up connection. The ISP realizes significant advantages because much of the existing Dial-up infrastructure (billing, authentication, security, etc.) can be used for DSL and other broadband services.

How do you connect to the Internet using PPPoE?

Along with a broadband modem, the ISP installs a software application on your computer that asks for a username and password. After this information is provided, the connection is established allowing the user to access the Internet.

What are some problems with PPPoE?

- Multiple accounts — The biggest problem using PPPoE without a Firewall is that the ISP requires the customer to have a PPPoE account for each computer attempting to access the Internet. The Firewall is able to manage PPPoE connections eliminating the need to install PPPoE software on each client machine.
- Home networking — Many home networking products don't support PPPoE, and if they do, configuration can be increasingly complex.
- Performance — There can also be a decrease in performance caused by the overhead required by PPPoE. In addition to sending the data and the Ethernet addresses and routing information, the PPPoE information must also be sent, adding to the overall bandwidth required for the transmission.

Can I have one PPPoE account for multiple computers in my home?

Yes. Using the PPPoE firmware, it is possible to have multiple computers share a single account from your service provider. This can save time and money in the set up and monthly fees of multiple PPPoE accounts.

IV

FIREWALL AND NETWORKING CONCEPTS

[Chapter 13](#) Types of Attack and Firewall Defences

[Chapter 14](#) Networking Concepts



13

TYPES OF ATTACK AND FIREWALL DEFENCES

This chapter describes the some of attacks that hackers may use to infiltrate and attack your network. It also details the way in which the Firewall will counter the attacks. The following sections are covered in this chapter:

- [Denial of Service Attacks](#)
- [Intrusion Attacks](#)
- [Trojan Horse Attacks](#)

Denial of Service Attacks

Denial of Service (DoS) attacks are malicious attacks designed to cause harm. The consequences of an attack range from the loss of few seconds of time on a web server or network to the crash of a server. In the worst case the attacker can learn enough about your company infrastructure and exploit its vulnerabilities to crash any server at will.

Denial of Service attacks work by exploiting weaknesses in TCP/IP, exploiting weaknesses in your servers or by generating large amounts of traffic (brute force attacks). Commonly attempted attacks and the reaction of the SuperStack® 3 Firewall are listed below.

Ping of Death

A *ping of death* attack attempts to crash your system by sending a fragmented packet which, when reconstructed is larger than the maximum allowable size. Other known variants of the *ping of death* include *teardrop*, *bonk* and *nestea*.

Firewall Response: Packet is dropped. Attack is stopped.

Smurf Attack

A *smurf attack* involves two systems. The attacker sends a packet containing a ICMP echo request (ping) to the network address of one system. This system is known as the amplifier.

The return address of the ping has been faked (spoofed) to appear to come from a machine on another network (the victim). The victim is then flooded with responses to the ping. As many responses are generated for only one attack, the attacker is able to use many amplifiers on the same victim.

The results of a *smurf attack* range from slowing of the network to the crashing of the victim devices.

Firewall Response as Amplifier: Spoofed IP address is detected and packet is dropped. Firewall does not act as amplifier.

Firewall Response as Victim: Traffic from a *smurf attack* cannot be separated from other network traffic. Traffic is allowed to pass.

SYN Flood Attack

A *SYN flood attack* attempts to slow your network by requesting new connections but not completing the process to open the connection. Once the buffer for these pending connections is full a server does not accept any more connections and is unresponsive.

Firewall Response: The connection request is completed by the Firewall and the connection monitored to check if data is sent. If no data is sent the Firewall resets the connection.

Land Attack

A *land attack* is an attempt to slow your network down by sending a packet with identical source and destination addresses originating from your network.

Firewall Response: Packet is dropped. Attack is stopped.

Intrusion Attacks

An *Intrusion Attack* is designed to get information from your network or place information on your network. This may be the theft of confidential material, the defacing of a web site or the theft of passwords or discovery of network infrastructure that will enable further attacks.

External Access

Without a firewall your network can be accessed from anywhere on the *Wide Area Network* (WAN) outside your network. The Firewall blocks all attempts to access the *Local Area Network* (LAN) that are initiated from outside your network

Firewall response: Packet is dropped. Attack is stopped.

Port Scanning Port Scanning is the testing of ports to see which are active and which are disabled. Although ports are scanned as part of normal traffic the scanning of many ports in a short period of time is a common precursor to an attack

Firewall Response: None - the Firewall allows *port scanning* but logs all port scans to aid diagnosis. Ports not in use are disabled by the Firewall.

IP Spoofing *IP Spoofing* is a method of masking the identity of an intrusion by making it appear that the traffic came from a different computer. This is used by intruders to keep their anonymity and can be used in a *Denial of Service* attack.

Firewall Response: The Firewall drops any spoofed packets, logs the event and alerts the administrator.

Trojan Horse Attacks

Trojan Horse attacks rely on a piece of software installed within your network prior to the attack. Attacks vary in severity and effect from showing messages on screen or crashing an individual PC to theft of information and infiltration of the network.

The *Firewall* blocks attacks in two ways:

- Known *Trojan Horse* attacks are identified and blocked.
- Ports not in use are blocked by default.

Trojan Horse attacks that the Firewall is capable of blocking include: *Back Orifice*, *ini killer*, *NetBus*, *NetSpy*, *Priority*, *Ripper*, *Senna Spy*, *Striker*, and *SubSeven*.



Using an anti-virus tool and updating the firmware of your Firewall as soon as a new version is available significantly increases your chance of resisting a Trojan Horse attack.

14

NETWORKING CONCEPTS

This appendix contains the following:

- [Introduction to TCP/IP](#)
- [Network Address Translation \(NAT\)](#)
- [Dynamic Host Configuration Protocol \(DHCP\)](#)
- [Port Numbers](#)
- [Virtual Private Network Services](#)
- [Bandwidth Management](#)
- [RADIUS Server Configuration](#)

Introduction to TCP/IP

Protocols are rules that networking hardware and software follow to communicate with one another. The Firewall uses the TCP/IP protocol.

IP and TCP

IP stands for Internet Protocol. This protocol provides connectionless data transfer over a TCP/IP network. Because IP alone does not provide end-to-end data reliability as well as some other services, other protocols such as TCP can be added to provide these services. TCP stands for Transmission Control Protocol. In TCP/IP, TCP works with IP to ensure the integrity of the data traveling over the network. TCP/IP is the protocol of the Internet.

IP Addressing

To become part of an IP network, a network device must have an IP address. An IP address is a unique number that differentiates one device from another on the network to avoid confusion during communication. To help illustrate IP addresses, the following sections compare an IP address to the telephone numbering system, a system that is used every day.

Like a phone number with a long distance number and area code, an IP address contains a set of four numbers. Where the components in phone numbers can be separated with dashes, for example, **1-408-555-1212**, IP address number components are separated by decimal points or dots (called *dotted decimal notation*), for example, **123.45.67.89**. Because computers use a binary number system, each number in the set must be less than 255.

There are three components that contribute to an IP address:

- IP address
- Subnet mask
- Default gateway

The following sections discuss each of these components in detail.

IP Address

Just as each household or business requires a unique phone number, a networked device (such as a computer, printer, file server, or router) must have a unique IP address. Unlike phone numbers, in IP addressing it is necessary to always use the entire number when communicating with other devices.

There are three classes of IP addresses: A, B, and C. Like a main business phone number that one can call and then be transferred through interchange numbers to an individual's extension number, the different classes of IP addresses provide for varying levels of *interchanges* or subnetworks and *extensions* or device numbers. The classes are based on estimated network size:

- Class A — used for very large networks with hundreds of subnetworks and thousands of devices. Class A networks use IP addresses between **0.0.0.0** and **127.0.0.0**.
- Class B — used for medium to large networks with 10–100 subnetworks and hundreds of devices. Class B networks use IP addresses between **128.0.0.0** and **191.0.0.0**.
- Class C — used for small to medium networks, usually with only a few subnetworks and less than 200 devices. Class C networks use IP addresses between **192.0.0.0** and **223.0.0.0**.

Just as you obtain a phone number from the phone company, there are controlling bodies for IP addresses. The overall controlling body for IP

addresses worldwide is InterNIC. Businesses or individuals can request one or many IP addresses from InterNIC; if you can estimate the future growth of the network, this can help you to work out the class and number of IP addresses you need.

Most large centralized companies have a network manager in charge of all IP address numbers. Other companies have a distributed administration scheme that allows the local network manager to set local IP addresses. In this case, the local manager gets a sub network or “interchange” number from the company’s central network manager and then assigns local IP address numbers.

Subnet Mask

As mentioned in [“IP Address”](#) on [page 216](#), the IP addressing system allows creation of subnetworks or *interchanges* and device numbers or *extensions* within those subnetworks. These numbers are created using a mathematical device called a subnet mask. A subnet mask, like the IP address, is a set of four numbers in dotted decimal notation. Subnet masks typically take three forms:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

The number 255 *masks* out the corresponding number of the IP address, resulting in IP address numbers that are valid for the network. For example, an IP address of **123.45.67.89** and a subnet mask of **255.255.255.0** results in a sub network number of **123.45.67.0** and a device number of **89**. The IP address numbers that are valid to use are those assigned by InterNIC; this prevents someone setting up IP addresses that are duplicates of those at another company.

The subnet mask used for the network typically corresponds to the class of IP address assigned. If the IP address is Class A, use a subnet mask of **255.0.0.0**. Class B addresses use a subnet mask of **255.255.0.0**, and Class C IP addresses use a subnet mask of **255.255.255.0**.

Default Gateway

A default gateway is like a long distance operator — users can dial the operator to get assistance connecting to the end party. In complex networks with many subnetworks, gateways keep traffic from traveling between different subnetworks unless addressed to travel there. While

this helps to keep overall network traffic more manageable, it also introduces another level of complexity.

To communicate with a device on another network, the message must go through a gateway that connects the two networks. Therefore, users need to know the default gateway's IP address. If there is no gateway in the network, use an IP address of 0.0.0.0 in fields that apply to a default gateway.

Network Address Translation (NAT)

Network Address Translation (NAT) is used to re-map all the addresses on a LAN to a single address on the Internet. This can be useful for three reasons:

- You may have a pre-existing LAN, not connected to the Internet, which uses invalid Internet addresses. NAT can be used to connect these machines to the Internet without changing all of their addresses.
- You may wish to obtain a single-user account from your Internet Service Provider instead of a LAN account, since single user accounts tend to be cheaper. NAT can be used to make all the machines on your LAN appear to be a single computer hooked up to the Internet.
- Additional security is provided when all the addresses on your network are invisible to the outside world.

If you wish to use addresses on your LAN, which have not been assigned to you by your Internet Service Provider, it is a good idea to use addresses in a special range allocated for this purpose. The following three blocks of IP address space have been reserved by the Internet Assigned Numbers Authority for the purpose of creating private internets:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

If you use some other arbitrary range, then there is the chance that the range is actually in use by someone else on the Internet. If this is the case, you will not be able to access their sites from your LAN.



If you reconfigure the IP addresses of the machines on your LAN, it is sometimes necessary to change their Default Gateway address as well.

Limitations of Using NAT

- NAT and Remote Access are not compatible features, since NAT hides machines on your LAN from the Internet. If NAT is on, the only machines on the LAN, which can be accessed, are those designated as “Public LAN Servers”; these are available to anonymous users on the Internet without authentication.
- Not All Applications lend themselves easily to address translation by NAT devices. Especially, the applications that carry IP Addresses inside the payload.
- NAT devices operate on the assumption that each session is independent. Application, such as H.323, that use one or more control follow-on sessions, require the use of an Application Level Gateway (ALG). The ALG helps interpret and translate the payload, so that it is prepared for follow-on data sessions.
- NAT increases the risk of mis-addressing. For example, the same local address may be bound to different global address at different times and vice versa.

For more information on NAT, see

<http://www.ietf.org/rfc/rfc2663.txt>

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol is a protocol that allows computers on a network to get TCP/IP settings from a centralized server. This configuration information includes elements such as IP Address, subnet mask, DNS server address, and so forth. Here's how it works:

A DHCP server provides a dynamic, “leased” address to a DHCP client. This means that the client can use the provided IP address for a certain period of time. The DHCP server cannot give this address to a different client during the lease period, thus ensuring that there are no address conflicts. When the lease expires, then the client may renew the lease. If it does not renew the lease (for instance, if it has been switched off), then the server may give the dynamic address to a different client.

The Firewall contains both a DHCP server and client. They are used for different purposes. The DHCP server can be used to provide machines on the LAN with configuration information. This can make it much easier to administer these machines, since individual hosts do not need to configure one-at-a-time. The Firewall's DHCP server also supports an older protocol called “BootP”.

The DHCP client is used in conjunction with Network Address Translation. The Firewall can use its DHCP client to automatically configure the Firewall WAN IP Address, WAN subnet mask, and other parameters. This can be useful for corporate Intranets, cable modem networks, or other environments where dynamic addressing is desirable.

Port Numbers

The port numbers are divided into three ranges:

- Well Known ports — those from 0 to 1023
- Registered ports — those from 1024 to 49151
- Dynamic or Private ports — those from 49152 to 65535

Well Known Port Numbers

The Well Known Ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA) <http://www.iana.org> and on most systems can only be used by system processes, or by programs executed by privileged users. Many popular services, such as Web, FTP, SMTP/POP3 e-mail, DNS and so forth operate in this range.

The assigned ports use a small portion of the possible port numbers. For many years the assigned ports were in the range 0–255. Recently, the range for the assigned ports managed by the IANA has been expanded to the range 0–1023.

Registered Port Numbers

The Registered Ports are not controlled by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users.

While the IANA cannot control uses of these ports, it does list uses of these ports as convenience.

The Registered Ports are in the range 1024–49151.

Visit <http://www.ietf.org/rfc/rfc1700.txt> for a list of IP port numbers.

Private Port Numbers

The Private Ports are not controlled or recorded by the IANA and are used in the development of new software and in bespoke programs which will be used by few users only.

The Private Ports are in the range 49152–65535.

**Virtual Private
Network Services**

This section contains the following:

- Introduction to Virtual Private Networks
- VPN Applications
- Basic Terms and Concepts

**Introduction to
Virtual Private
Networks**

Virtual Private Networks (VPN) provide an easy, affordable, and secure means for businesses to conduct operations and provide network connectivity to all offices and partners. Using 3Com's intuitive Web interface, a secure connection may be established between two or more sites.

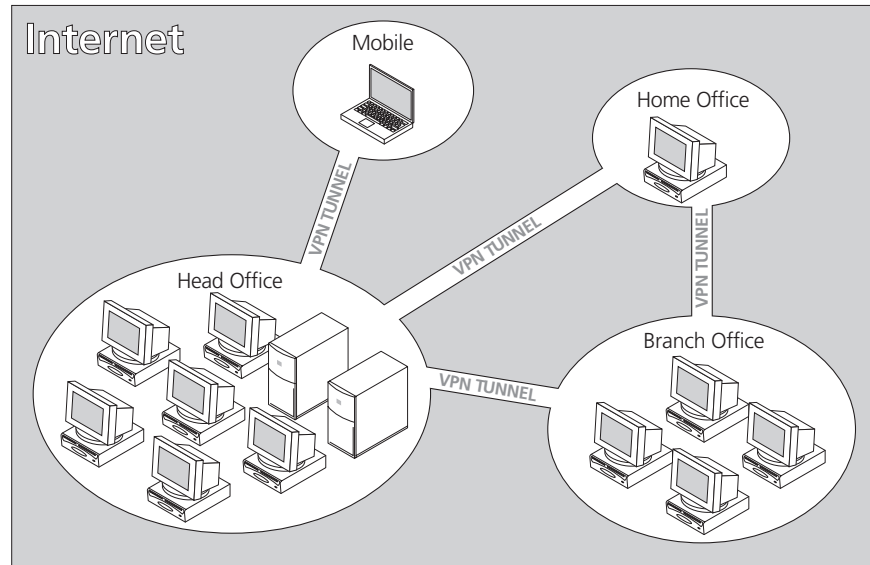
Data that is intended for delivery to a remotely connected site is automatically encrypted using the VPN's accelerated cryptographic processor. The data is delivered via the Web and decrypted at the intended destination.

The SuperStack 3 Firewall VPN implementation uses the IPSec VPN standard. This guarantees compliance with other VPN products, such as 3Com OfficeConnect Cable/DSL Secure Gateway and Check Point Firewall-1 that adhere to the same standard.

The SuperStack 3 Firewall supports up to 1001 Security Associations. Of these SAs, 1000 support a single site-to-site or client VPN tunnel, while the remaining single SA can support up to 1000 concurrent client VPN tunnels. This is called the *GroupVPN* SA. If you only have VPN client connections, you need only use the GroupVPN SA. However you will need to configure a separate SA for each site-to-site connection

VPN Applications

The following illustration shows the VPN connections between the offices and users of a simple company. In this example all external connections are made using VPN tunnels across the Internet.

Figure 76 Virtual Private Networks Applications

- *Linking two or more Private Networks Together*

VPN is the perfect way to connect branch offices and business partners to the primary business. Using VPN over the Internet, instead of leased site-site lines, offers significant cost savings and can improve performance.

- *Using the IRE VPN Client for Secure Remote Management*

Using the included IRE VPN client for Windows, a secure, encrypted tunnel may be created that allows the administrator to remotely manage the Firewall over the Internet.

- *Using L2TP Clients*

Microsoft is promoting L2TP/IPSec as the standard VPN client and introduced both IPSec support and L2TP in Windows 2000 as separate components. Windows XP provides an integrated L2TP/IPSec client. Microsoft has also released a free integrated L2TP/IPSec client for Windows 98, NT and ME. Version 6.3.0 and later of the SuperStack 3 Firewall firmware supports an L2TP/IPSec server and can make use of the Microsoft L2TP/IPSec clients.

- *Accessing Machines Using Private Addressing behind NAT*

When NAT (Network Address Translation) is enabled, remote users are not able to access hosts on the LAN unless the host is designated a

Public LAN Server for that specific protocol. Since the VPN Tunnel terminates inside the LAN, remote users can access all computers that use private IP addresses on the LAN.

Basic VPN Terms and Concepts

The following explains the most common terms and expressions used in VPN

- *VPN Tunnel*

Tunnelling is the encapsulation of point-point transmission inside IP packets. A VPN Tunnel is a term that is used to describe a connection between two or more private nodes or LANs over a public network, typically the Internet. Encryption is often used to maintain the confidentiality of private data when travelling over the Internet.

- *Encryption*

Encryption is a mathematical operation that transforms data from "clear text" (something that a human or a program can interpret) to "cipher text" (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric "key" be supplied along with the clear text. The key and clear text are processed by the encryption operation which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is the mathematical operation that transforms cipher text to clear text. Decryption also requires a key.

- *Key*

A key is an alphanumeric string that is used by the encryption operation to transform clear text into cipher text. Keys used in VPN communications can range in length, but are typically 16 or 32 characters. The longer the key, the more difficult it is to break the encryption. The reason for this is most methods used to break encryption involve trying every possible combination of characters, similar to trying to open a safe when the combination is not known.

- *Asymmetric vs. Symmetric Cryptography*

Asymmetric and symmetric cryptography refer to the keys used to authenticate, or encrypt and decrypt the data.

Asymmetric cryptography does not use the same key to verify the data. Asymmetric cryptography is often referred to as public key cryptography. With public key, each user gets a pair of keys, one called the public key and the other called the private key. The private key is always linked mathematically to the public key to be kept secret. All

communications involve only public keys; the private key is never transmitted or shared, but used to decrypt the message. A user can generate their own keys using key generation software, or have keys generated by trusted organizations. Once a key has been generated, the user must register his or her public key with a central administration, called a Certifying Authority (CA). Organizations, such as RSA Data Security and Verisign, can help users issue and register key pairs.

The Firewall VPN uses Symmetric Cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- *Authentication Header (AH)*

The Authentication Header is a mechanism for providing strong integrity and authentication for IP packets. Confidentiality and protection from traffic analysis are not provided by the Authentication Header.

The IP Authentication Header provides security by adding authentication information to an IP packet. This authentication information is calculated using all header and payload data in the IP packet. This provides significantly more security that is currently present in IP.

Use of AH increases the processing requirements in the Firewall and also increases the communication latency. The increased latency is primarily due to the calculation and comparison of the authentication data by the receiver for each IP packet containing an Authentication Header.

- *Data Encryption Standard (DES)*

When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. 3Com's implementation of DES uses a 56-bit key.

3Com's DES Key must be exactly 16 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

- *Strong Encryption (Triple DES or 3DES)*

Strong Encryption, or Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is dramatically more secure than DES, and is considered to be virtually unbreakable by security experts. It also

requires a great deal more processing power, resulting in increased latency and decreased throughput.

The 3DES Key must be exactly 24 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

- *ARCFour*

ARCFour (ARC4) is used for communications with secure Web Sites using the SSL protocol. Many banks use a 40-bit key ARC4 for online banking while others use a 128-bit key. 3Com's implementation of ARCFour uses a 56-bit key.

ARCFour is faster than DES for several reasons. First is that it is a newer encryption mechanism than DES. As a result, it benefits from advances in encryption technology. Second, unlike DES, it is designed to encrypt data streams, rather than static storage. DES has achieved much of its popularity because it is well known and has been proven to be very robust. ARCFour, while theoretically as secure as 56bit DES, does not have the long history that leads to the wide acceptance by security professionals.

3Com's ARCFour Key must be exactly 16 characters long and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

- *Security Parameter Index (SPI)*

The SPI is used to establish a VPN tunnel. The SPI is transmitted from the remote Firewall to the local Firewall. The local Firewall then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

The SPI must be unique, is from one to eight characters long, and is comprised of hexadecimal characters. Valid hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.



The range from "0" to "ff" inclusive, is reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. They are not accepted by the Firewall when entered as an SPI; an error message is displayed at the bottom of the Web browser window when the Update button is pressed.

- *Security Association (SA)*

A Security Association is the group of security settings relating to a given network connection or set of connections. The Security

Association is based on the SPI, and includes the Destination Address Range, IPSec gateway Address, Encryption method, Encryption Key and Authentication Key.

IPSec Protocol IPSec (IP security) is a set of protocols and mechanisms that secure and authenticate IP traffic. The main component of IPSec is Encapsulating Security Payload (ESP - IP protocol number 51) which is typically used to secure and authenticate the IP payload.

ESP uses encryption algorithms such as DES and 3DES to secure the traffic and uses message digest algorithms such as SHA and MD5 to authenticate the traffic.

IKE (Internet Key Exchange) is used to negotiate the keying material that is used by these encryption and authentication algorithms. IKE uses UDP port number 500 and precedes the actual IPSec data flow.

It is important for VPNs to work that UDP port number 500 and IP protocol number 51 are allowed through to the Firewall. The Internet router that the SuperStack 3 Firewall is connected to may require to be reconfigured to allow this particular traffic through.

Depending on how it is being used, IPSec can run in two modes:

- Tunnel mode
- Transport mode

IPSec Tunnel Mode

IPSec tunnel mode encapsulates and secures complete IP packets. It is typically used to provide site-to-site VPN connections in conjunction with IPSec gateway devices. These devices, such as the SuperStack 3 Firewall, tunnel the packets from one host on a private LAN across the Internet to a peer device that terminates the VPN tunnel and forwards the unencapsulated packets to a host on the remote private LAN.

Since complete packets are encapsulated, the private LANs do not need to use Internet routable IP addresses as the private IP addresses are hidden within the IPSec tunnel mode packets.

The Safenet VPN client uses IPSec tunnel mode to establish a VPN tunnel with the SuperStack 3 Firewall. A pseudo-standardized authentication mechanism called Extended Authentication (XAUTH) provides a means to

authenticate users when using IPSec tunnel mode. The SuperStack 3 Firewall and Safenet VPN client support XAUTH.

IPSec Transport Mode

IPSec transport mode encapsulates and secures only the data payload of IP packets. It is used to allow secure communications between hosts without requiring IPSec gateway devices.

As only the data portion of the packet is secured (instead of the full IP packet), the two hosts require publicly routable IP addresses to communicate with each other over the Internet.

L2TP Protocol

Layer 2 Tunnelling Protocol (L2TP) is a mechanism that provides a PPP (Point-to-point Protocol) connection between a user and a terminating device over an IP network. PPP is the protocol that is typically used to allow a dial-up user to connect to the Internet, authenticate and obtains his IP configuration.

L2TP allows the PPP protocol to be used over the Internet itself to allow a user to authenticate with a L2TP termination device and obtain appropriate IP configuration to access the private LAN behind the L2TP terminator.

As PPP contains mechanisms to provide security and authentication, L2TP can be used on its own to provide this *virtual* dial-up capability. However, when used with IPSec - L2TP/IPSec, much better security and authentication is provided. When secured with IPSec, L2TP uses IPSec transport mode as both the VPN client and L2TP terminator have a public IP address.

After completing the IPSec connection between the client and the Firewall, an L2TP tunnel is established and the PPP connection within L2TP authenticates the VPN client user and provides the VPN client with an appropriate *local* IP address.

The PPP connection encapsulates complete IP packets and hence the VPN client can communicate with the hosts on the private LAN that are not using public IP addresses. L2TP is only used for individual VPN clients. As with previous versions of the SuperStack 3 firmware, site-to-site connections continue to use IPSec tunnel mode.

Bandwidth Management

This section provides an overview of the bandwidth management function that can be implemented as part of:

- Ethernet Port Configuration
- VPN Configuration
- Policy Rules

Bandwidth is the capacity of a communication channel (for example, cable, DSL, T1 lines) to carry signals. A larger bandwidth can transfer more data over a communication channel in a given time. Sometimes this is referred to as throughput. In digital communications this is measured in bits per second (bps) or a multiple of bps such as Kbps, Mbps or Gbps.

Bandwidth Management is a means of allocating bandwidth resources to critical applications on your network. Without bandwidth management, an application or a user can take control of all available bandwidth and prevent other applications or users from using the network. Because it is impossible to differentiate between types of network traffic, it is also impossible to control which users or applications have priority on the network.

Applications can also require a specific quantity and quality of service which cannot be predicted in terms of available bandwidth. This can make some applications run poorly if bandwidth is not properly allocated to the application when necessary.

Bandwidth management works by sorting outbound network traffic into classes by application and service type. Traffic is then scheduled according to the minimum and maximum bandwidth configured for each traffic type.

Why Use Bandwidth Management?

Corporate networks using intranets for information sharing and Web navigation have an increased demand for bandwidth, but simply adding on more or larger connections (such as T1 lines) doesn't address the bandwidth issue sufficiently because network availability is still not guaranteed.

Nearly all network links are shared by more than one user or application which means available bandwidth is shared between all users and all applications. Using bandwidth management to allocate bandwidth to applications or to specific users at peak times can prevent traffic congestion on the network. Temporary network congestion can be improved by using bandwidth management.

The Firewall and Bandwidth Management

The Firewall implements bandwidth management on outbound traffic only. It allows network administrators to guarantee minimum bandwidth and prioritize traffic based on Rules created in the *Policy* section of the Web interface. By controlling the amount of bandwidth available to an application or a user, the network administrator can prevent a small number of applications or users consuming all the available bandwidth.

Key Features

- Outgoing traffic is managed according to traffic type: Telnet, FTP, HTTP etc.
- Network Access Rules can be configured to allocate bandwidth based on IP addresses.
- VPN traffic can also be managed by enabling bandwidth management on the VPN Configure tab and the specifying the Guaranteed, Maximum, and priority of all VPN traffic through the Firewall.



Bandwidth management cannot be configured for individual VPN Security Associations. It can only be configured for all VPN traffic.

Key Benefits

- You have full control of outbound network traffic and can prevent traffic congestion on the network.
- You can prevent a small number of applications and users consuming all available bandwidth.
- You can implement Quality of Service policies across the network allowing business critical and other priority applications to run smoothly.

How Does It Work?

Bandwidth management in the Firewall works by allocating traffic to a class based upon application type, source or destination address, or a combination of both. It then assigns individual limits for each class of network traffic. As each type of network traffic is then prioritized, applications that require a quick response time, such as Telnet, can take precedence over traffic tolerant of a slower response time, such as FTP.

Balancing bandwidth allocated to different network traffic and the assigning priorities to traffic can improve your network's performance.

Traffic is classified as follows:

- TCP/IP or UDP ports
- Services such as FTP, HTTP, E-Mail, SIP
- Source or destination IP addresses

The Firewall's bandwidth management can assign a portion of the available bandwidth and a priority to each class of network traffic. Priorities rank from 0 (zero), the highest, to 7, the lowest.

The Firewall's packet classifier analyzes a packet when it arrives at the Firewall to check for the protocol, source information and destination information. It then allocates the packet to a class queue where it waits to be processed. If the queue is full, the packet is dropped. Normal retransmission of data ensures that the packet is sent again.

Class queues are processed based on the amount of bandwidth allocated (guaranteed and maximum) and the priority assigned to the class queue. Within the class queue, packets processed on a first-in first-out basis. When the network traffic reaches the maximum allocated to the class, packets from the next class in priority order are processed.

Typically, each class is allocated a portion of the available bandwidth and when that limit is reached, no more traffic for that particular class is forwarded. However, if there is available bandwidth on the network that is not in use by a particular class, a class can temporarily *borrow* bandwidth and send traffic until the maximum bandwidth allocated to the class is reached.

Spare bandwidth is allocated among the high priority classes until no more bandwidth is available or until all of those classes have reached their maximum bandwidth. If this happens, the remainder of the bandwidth is divided amongst the next priority classes. This process is repeated until all of the available bandwidth is consumed.

Defining a class of traffic that has 0 bandwidth allocated to it, effectively blocks the traffic unless there is no other traffic with higher priority on the network.

Enabling Bandwidth Management

To enable Bandwidth Management on the Firewall, you must know the current bandwidth of your connection. Once you know this open the Web interface and select *Advanced* and then *Ethernet*. Then check the Enable Bandwidth Management box and enter the amount of available WAN bandwidth in Kbps. Now that you have enabled bandwidth management, you can configure Rules to use bandwidth management.

Table 9 Examples of Bandwidth Management Rules

Rule	Service	Priority	Guaranteed	Maximum
Allow	SMTP	0 (highest)	300 Kbps	1000 Kbps
Allow	FTP	1	100 Kbps	200 Kbps
Allow	HTTP	2	100 Kbps	200 Kbps

RADIUS Server Configuration

Individual users must have their privileges defined on the RADIUS server used for authenticating the users. Global user privileges can be configured on the *RADIUS* tab of the Firewall's Web interface, but Firewall-specific privileges must be configured on the RADIUS server.

Different vendors also have different methods of configuring the privileges on their servers. In some cases, it can be complex, but most allow for the configuration of group profiles or policies which means you can configure the attributes once per group. This section describes the configuration of user privileges on various vendors of RADIUS servers, and also notes the particular RADIUS servers which support CHAP (Challenge Handshake Authentication Protocol) mode. CHAP support is required if HTTPS is not available for logging into the Firewall.

Steel Belted RADIUS from Funk Software

Steel Belted RADIUS server version 3.0 from Funk Software supports pre-configuration of vendor-specific attributes in a vendor-specific dictionary file. *ss3-Firewall.dct* is the new dictionary file for the Firewall. This file can be found on the CD-ROM accompanying your Firewall or can be obtained from <http://www.3Com.com/ssfirewall> in the *Downloads* section.



Refer to your Steel Belted RADIUS Administration Guide for complete instructions on adding dictionaries and configuring user privileges.

To configure the Steel Belted RADIUS server to include the `SS3-Firewall.dct` file, carry out the following:

- 1 Locate the directory that Steel Belted RADIUS is installed, `C:\RADIUS` by default, and copy the `SS3-Firewall.dct` file into `C:\RADIUS\Service` folder.
- 2 Edit the `vendor.ini` file located in the Service folder using Notepad. Add the following lines so that they are in alphabetical order with the other vendor products in the file.


```
vendor-product = SS3-Firewall
dictionary = SS3-Firewall
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```
- 3 Edit the `dictionary.dcm` file using Notepad, and add the entry **@SS3-Firewall.dct** to it, keeping the entry in alphabetical order with the existing entries.
- 4 Restart the Windows service called `Steel Belted RADIUS Service`.
- 5 Run the `Steel Belted RADIUS Administrator`.
- 6 Click *RAS Clients*, and select *SS3-Firewall* from the *Make/Model* list. Click *Save*.



If there is no entry for SS3-Firewall, be sure that steps 2 and 3 were performed correctly.

Configuring User Privileges

To configure user privileges, follow these steps:

- 1 With *Steel Belted RADIUS Administrator* open, click *Users* and select the User to configure. Or select a profile to be configured from the *Profile Name* menu.
- 2 Click *Ins* and select *SS3-Firewall-User-Privilege* from the *Available Attributes* list.
- 3 Select the privilege to be set, and click *Add*. Repeat until all of the privileges are added for the user. Steel Belted RADIUS does support CHAP, so authentication takes place even if HTTPS is not available when logging into the Firewall's Web interface. Select *Allow PAP or CHAP* when setting user passwords.

ACE Server from RSA The ACE Server, version 4.1, from RSA configures RADIUS attributes into the profiles. It does not support pre-configuration of vendor-specific attributes on the server. It also only allows one vendor-specific attribute to be set per profile, and only support vendor-specific attributes containing ASCII text. User privileges are added manually as follows:

- 1 Open the *ACE Server Database Administrator* program.
- 2 Select *Edit Profiles* from the menu, and select the profile to be configured with user privileges. Click *OK*.
- 3 From the *Available Attributes* menu, select *Vendor-Specific*, and then click *Add Attribute*.
- 4 Set the value to **8741 2 "privileges-list"** where privileges list is a comma-separated list of 2-letter privileges, as follows:

RA — Remote Access

BF — Bypass Filters

VC — Access from VPN Client

VA — Access to VPNs

LM — Limited Management

LC — Access from L2TP VPN Client

For example, to configure a profile with Access to VPN privileges and allow Access from VPN Client, the value is set as follows:

8714 2 "VA, VC"

The ACE Server from RSA does not support CHAP with RADIUS, therefore it is necessary to configure the Firewall to use HTTPS when logging into the Firewall's Web interface.

**Internet
Authentication
Service on Microsoft
Windows NT/2000
Server**

The RADIUS server used on Microsoft Windows NT and Windows 2000 servers is known as the Internet Authentication Service (IAS). The RADIUS attributes are configured using policies, and does not support pre-configuration of vendor-specific attributes. The RADIUS attributes are entered manually into the service as follows:

- 1 Open *IAS*, and select *Remote Access Policies*.
- 2 Select the policy to be configured for user privileges, and right click. Select *Properties* from the list.

- 3 Click *Edit Profile*, and then click *Advanced*. Click *Add*.
- 4 Select *Vendor-Specific* from the list, and click *Add*. The *Multivalued Attribute Information* box appears.
- 5 Click *Add*. The *Vendor-Specific Attribute Information* box appears.
- 6 Click *Enter Vendor Code*, and enter *8741* as the vendor code.
- 7 Click *Yes, It conforms*, and then click *Configure Attribute*. The *Configure VSA (RFC compliant)* window appears.
- 8 Enter *1* as the *Vendor-assigned attribute number*.
- 9 Select *Decimal* as the *Attribute format*.
- 10 Enter one of the following values as the *Attribute* value. Each value defines a privilege for users within the policy.
 - 1 — Remote Access
 - 2 — Bypass Filters
 - 3 — Access from VPN Client
 - 4 — Access to VPNs
 - 5 — Limited management
 - 6 — Access from L2TP VPN Client
- 11 Click *OK*, and then *OK* again to return to the *Multivalued Attribute Information* window.
- 12 Repeat Steps 5 through 11 for each privilege configured for a policy.

For further information, refer to *To configure vendor-specific attributes for a remote access policy* in the IAS help file. With IAS, the user database is located on the domain controller. Therefore, IAS only supports CHAP with RADIUS if the domain controller is configured to store passwords using reversible encryption for all users. If the domain controller is not configured in this manner, it is necessary to use HTTPS to log into the Firewall's Web interface.

RADIUS Attributes Dictionary

This is the RADIUS dictionary file (ss3_Firewall.dct) for the Firewall. It can be found on the CD-ROM accompanying the Firewall or on the 3Com Web site at <http://www.3com.com/ssfirewall>. Follow the *Downloads* link.

```
#####~#####
# SS3-Firewall.dct      - This is the RADIUS dictionary File for the 3Com
#                      SuperStack 3 Firewall.
#
#####

#
# Start with the Standard RADIUS specification attributes
#
@radius.dct

MACRO SS3-VSA(type,syntax)26 [vid=8741 type1=%type% len1=+2 data=%syntax%]

ATTRIBUTE SS3-Firewall-User-Privilege SS3-VSA(1, integer) R
VALUE      SS3-Firewall-User-Privilege Remote-Access      1
VALUE      SS3-Firewall-User-Privilege Bypass-Filters      2
VALUE      SS3-Firewall-User-Privilege VPN-Client-Access    3
VALUE      SS3-Firewall-User-Privilege Access-To-VPN        4
VALUE      SS3-Firewall-User-Privilege Limited-Management   5
VALUE      SS3-Firewall-User-Privilege L2TP-Client-Access    6

# ATTRIBUTE SS3-Firewall-User-Privileges SS3-VSA(2, integer) R
#
# This is a text string giving a comma-separated list of one or more privileges
# (each corresponds to a value of the SS3-Firewall-User-Privilege attribute
# above):
# "RA,BF,VC,VL,LM,LC"
#
# This attribute is to use in place of SS3-Firewall-User-Privilege with RADIUS
# servers that allow only one instance of a Vendor-Specific attribute to be
# set (such as the ACE Server from RSA). Note that it is commented out in this
# file because it is not needed in any servers that support this file format.

#####
# End of SS3-Firewall.dct - This is the RADIUS dictionary file for the 3Com
#                      SuperStack 3 Firewall.
#####
```


V

APPENDICES

Appendix A	Safety Information
Appendix B	Technical Specifications and Standards
Appendix C	Cable Specifications
Appendix D	Technical Support
	Index
	Regulatory Notices



A

SAFETY INFORMATION



WARNING: Please read the 'Important Safety Information' section before you start.



VORSICHT: Bitte lesen Sie den Abschnitt 'Wichtige Sicherheitsinformationen' sorgfältig durch, bevor Sie das Gerät einschalten.



AVERTISSEMENT: Veuillez lire attentivement la section 'Consignes importantes de sécurité' avant de mettre en route.

Important Safety Information



WARNING: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully. You must read the following safety information carefully before you install or remove the unit:



WARNING: Exceptional care must be taken during installation and removal of the unit.



WARNING: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.



WARNING: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.



WARNING: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.



WARNING: There are no user-replaceable fuses or user-serviceable parts inside the unit. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.



WARNING: Disconnect the power adapter before moving the unit.



WARNING: RJ-45 Ports. These are shielded RJ-45 data sockets. They cannot be used as standard traditional telephone sockets, or to connect the unit to a traditional PBX or public telephone network. Only connect RJ-45 data connectors, network telephony systems, or network telephones to these sockets. Either shielded or unshielded data cables with shielded or unshielded jacks can be connected to these data sockets.

Wichtige Sicherheitshinweise



VORSICHT: Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.



VORSICHT: Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Gerät installieren oder ausbauen:



VORSICHT: Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.



VORSICHT: Stapeln Sie das Gerät nur mit anderen SuperStack 3 Gerätes zusammen.



VORSICHT: Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.



VORSICHT: Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.



VORSICHT: Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.



VORSICHT: Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Switch haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.



VORSICHT: Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.



VORSICHT: RJ-45-Porte. Diese Ports sind geschützte Datensteckdosen. Sie dürfen weder wie normale traditionelle Telefonsteckdosen noch für die Verbindung der Einheit mit einem traditionellen privatem oder öffentlichem Telefonnetzwerk gebraucht werden. Nur RJ-45-Datenanschlüsse, Telefonnetzsysteme oder Netztelefone an diese Steckdosen anschließen. Entweder geschützte oder ungeschützte Buchsen dürfen an diese Datensteckdosen angeschlossen werden.

Consignes Importantes de Sécurité



AVERTISSEMENT: Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes. Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d'installer ou de retirer l'appareil:



AVERTISSEMENT: Faites très attention lors de l'installation et de la dépose du groupe.



AVERTISSEMENT: Seulement entasser le moyeu avec les autres moyeux SuperStack 3.



AVERTISSEMENT: Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l'adaptateur électrique remis avec cet appareil.



AVERTISSEMENT: La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.



AVERTISSEMENT: L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.



AVERTISSEMENT: Il n'y a pas de parties remplaçables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.



AVERTISSEMENT: Débranchez l'adaptateur électrique avant de retirer cet appareil.



AVERTISSEMENT: Points d'accès RJ-45. Ceux-ci sont protégés par des prises de données. Ils ne peuvent pas être utilisés comme prises de téléphone conventionnelles standard, ni pour la connection de l'unité à un réseau téléphonique central privé ou public. Raccorder seulement connecteurs de données RJ-45, systèmes de réseaux de téléphonie ou téléphones de réseaux à ces prises.
Il est possible de raccorder des câbles protégés ou non protégés avec des jacks protégés ou non protégés à ces prises de données.

B

TECHNICAL SPECIFICATIONS AND STANDARDS

This appendix lists the technical specifications for the SuperStack 3 Firewall. The Firewall has been designed and certified to the following standards:

Table 10 Technical Specifications of the Firewall

Physical

Width: 440 mm (17.3 in.)

Depth: 230 mm (9.0 in.)

Height: 44 mm (1.7 in.) or 1 U

Weight: 2.55 kg (5.6 lb)

Mounting: Free standing, or 19in. rack mounting using the mounting kit supplied

Capacity

Maximum Number of Simultaneous IP Connections: 30,000

Maximum Number of Security Associations: 1,001

Maximum Number of VPN Tunnels: 1,000

Size of DHCP pool: 255 bindings

Maximum Number of Rules: 100

Maximum Number of Custom Services: 64

AC Line Frequency

50-60Hz

Current Rating (max): 3.15A

Input Voltage: 90-264Vrms

Operating Temperature

0-50 °C (32-122 °F)

Humidity

10-95% (non-condensing)

Electrical Interfaces

Three 10/100 BASE-T RJ45 Connectors

Table 10 Technical Specifications of the Firewall

Functional
ISO/IEC 8802-3, IEEE 802.3
Safety
UL1950, EN 60950, CSA 22.2 #950, IEC 950
EMC
EN55022 Class A, EN 50082-1, FCC Part 15 Part Class A, ICES-003 Class A, VCCI Class A, EN 55024, CNS 13438 Class A
Environmental
EN 60068 (IEC 68)
HTTPS Management
Supports the following versions of SSL: SSLv2, SSLv3, and TLSv1. Also, the following encryption ciphers are supported: RC4-MD5, EXP-RC4-MD5, DES-CBC3-SHA, DES-CBC-SHA, RC4-SHA, EXP-RC2-CBC-MD5, NULL-SHA, and NULL-MD5. The RSA key used is 1024-bit.
Power Inlet
IEC 320

C

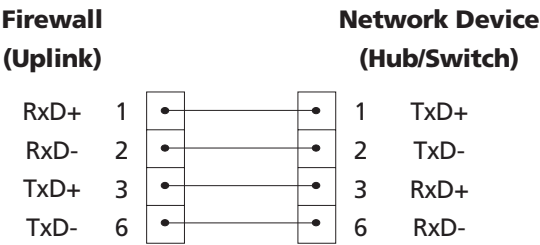
CABLE SPECIFICATIONS

Cable Specifications The Firewall supports the following cable types and maximum lengths:

- Category 5 cable.
- Maximum cable length of 100 m (327.86 ft).

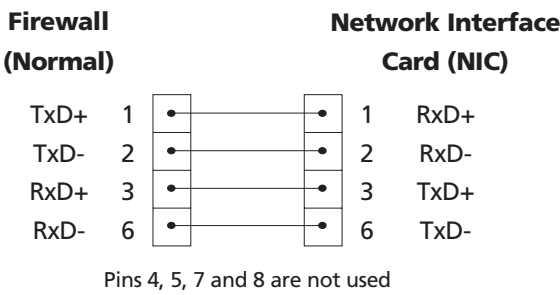
Pinout Diagrams [Figure 77](#) and [Figure 78](#) show the pin connections when using a straight through Category 5 cable. This is the standard cable used for Ethernet and Fast Ethernet.

Figure 77 Connecting the Firewall to a hub or switch using a straight through cable



Pins 4, 5, 7 and 8 are not used

Figure 78 Connecting the Firewall to a Network Interface Card using a straight through cable



[Figure 79](#) and [Figure 80](#) show the pin connections when using a crossover Category 5 cable. It is not necessary to use a crossover cable with your Firewall as the Normal/Uplink switch beside each port serves the same purpose.

Figure 79 Connecting the Firewall to a hub or switch using a crossover cable

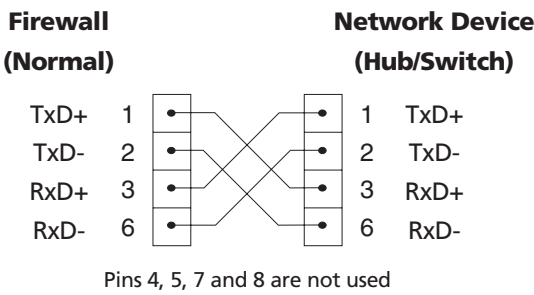
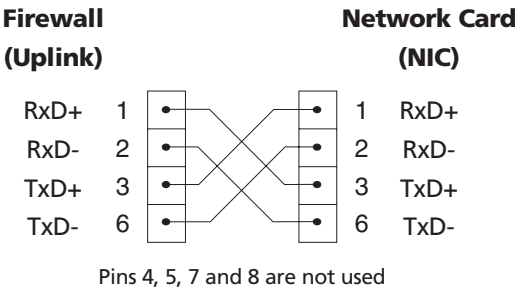


Figure 80 Connecting the Firewall to a network interface card using a crossover cable



D

TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

<http://www.3com.com/>

This service provides access to online support information such as technical documentation and software, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

The 3Com Knowledgebase is a database of technical information to help you install, upgrade, configure, or support 3Com products. The Knowledgebase is updated daily with technical information discovered by 3Com technical support engineers. This complimentary service, which is available 24 hours a day, 7 days a week to 3Com customers and partners, is located on the 3Com Corporation World Wide Web site at:

<http://knowledgebase.3com.com>

3Com FTP Site Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**



You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers email and telephone technical support services. To find out more about your support options, email or call the 3Com technical support services at the location nearest you.

Email Support Some 3Com regions offer an email support service. To access this service for your region, use the appropriate URL or email address from the list below.

Asia, Pacific Rim

From this region, email:

`apr_technical_support@3com.com`

Europe, Middle East and Africa

From this region, enter the URL:

`http://emea.3com.com/support/email.html`

Latin America

Spanish speakers, enter the URL:

`http://lat.3com.com/lat/support/form.html`

Portuguese speakers, enter the URL:

`http://lat.3com.com/br/support/form.html`

English speakers, email:

`lat_support_anc@3com.com`

Telephone Support When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers. These numbers are correct at the time of publication. Refer to the 3Com Web site for updated information.

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim			
Australia	1 800 678 515	Philippines	1235 61 266 2602 or +61 2 9937 5076
Hong Kong	800 933 486	P.R. of China	10800 61 00137 or 021 6350 1590 or 00800 0638 3266
India	+61 2 9424 5179 or 000800 650 1111		800 6161 463
Indonesia	001 803 61009		00798 611 2230 or 02 3455 6455
Japan	00531 616 439 or 03 5977 7991	Singapore	00801 611 261
Malaysia	1800 801 777	S. Korea	001 800 611 2000
New Zealand	0800 446 398	Taiwan	
Pakistan	+61 2 9937 5083	Thailand	
Europe, Middle East and Africa			
From anywhere in these regions, call:	+44 (0)1442 435529		
From the following countries, you may use the numbers shown:			
Austria	01 7956 7124	Luxembourg	800 29880
Belgium (Flemish)	070 700 000	Netherlands	0900 777 7737
Belgium (French)	070 700 770	Norway	815 33 047
Denmark	7010 7289	Poland	00800 441 1357
Finland	01080 2783	Portugal	707 200 123
France	0825 809 622	South Africa	0800 991196
Germany	01805 404 747	Spain	9 021 60455
Hungary	06800 14466	Sweden	07711 14453
Ireland	1800 509359	Switzerland	08488 50112
Israel	1800 943 2632	U.K.	0870 241 3901
Italy	199 161346		
Latin America			
Antigua	1 800 998 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888
North America	1 800 876 3266		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

You can obtain an authorization number (called an RMA) by entering the following URL into your Internet browser:

http://www.3com.com/support/en_US/repair

Alternatively, you can obtain an RMA by calling or faxing one of the following numbers:

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim			
From anywhere in this region call:	+ 65 543 6500 phone + 65 543 6348 fax		
Europe, Middle East and Africa			
From anywhere in these regions, call:	+44 (0)1442 435529		
From the following countries, you may use the numbers shown:			
Austria	01 7956 7124	Luxembourg	800 29880
Belgium (Flemish)	070 700 000	Netherlands	0900 777 7737
Belgium (French)	070 700 770	Norway	815 33 047
Denmark	7010 7289	Poland	00800 441 1357
Finland	01080 2783	Portugal	707 200 123
France	0825 809 622	South Africa	0800 991196
Germany	01805 404 747	Spain	9 021 60455
Hungary	06800 14466	Sweden	07711 14453
Ireland	1800 509359	Switzerland	08488 50112
Israel	1800 943 2632	U.K.	0870 241 3901
Italy	199 161346		

Country	Telephone Number	Country	Telephone Number
Latin America			
Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888
North America			
	1 800 876 3266 phone		
From U.S.A and Canada call:	1 508 323 6061 fax (not toll free)		

INDEX

Numbers

0.0.0.0 218
10 Mbps
 status LED 34
100 Mbps
 status LED 34
10BASE-T cable
 DMZ connection 38
 LAN connection 38
255.255.255.0 217
3Com Knowledgebase Web Services 247
3Com Network Supervisor 23
3Com URL 247

A

acceptable use policy 88, 104
access
 remote 28
ActiveX
 blocking 97
 defined 81
add route 145
adding a service 116
administrator
 authenticating 200
 password 60, 200
advanced redundant power supply 36
alert LED 35
alerts 27, 95
ARPS 36
attacks, DoS 25
authenticated management session 127
authentication
 updating users 126
automatic IP address sharing and configuration 28
automatic LAN settings 51
automatic WAN settings 45

B

bandwidth usage
 by IP address 104

 by service 104
blocking categories 85, 97
broadband modems 28

C

cable specifications 245
clock, setting 61
CMT 17
code archive blocking 97
configuration
 saving and restoring 106
consent 88
 URL 89
conventions
 notice icons, About This Guide 14
cookies 81
current sample period 103
custom list 85
 options 87
CyberNOT list 189
 reviewers 189

D

data collection, starting 103
default
 gateway 217
 password 200
default IP address, Firewall 42
default policies
 diagram 37
deleting
 services 118
 users 127
Demilitarised Zone Port 15
demilitarized zone port 22
Denial of Service Attacks 15
Denial of Service attacks
 IP Spoofing 25
 LAND Attack 25
 Ping of Death 25
 SYN Flood 25
 Teardrop 25

DHCP
 client 28
 overview 28
 DHCP server
 setting up 69
 viewing status 75
 diagnostic tools 76
 diagram 35
 direct connection 201
 disable web proxy 82
 display report 104
 DMZ addresses, specifying 67
 DMZ Port 15
 DMZ port 22
 attaching Internet servers to 38
 DNS Name Lookup Tool 76
 DoS Attacks 15
 DoS attacks 25

E
 E-Mail, feedback 17
 events 95
 export file, specifying 108
 export settings 108
 before updating the software 109

F
 factory defaults, restoring 108, 198
 features
 automatic IP address sharing and
 configuration 28
 firewall security 25
 Internet filtering 26
 logs and alerts 27
 user remote access 28
 filter list
 updating 83
 filter settings 79
 filtering
 web 26
 filters, specifying when they apply 87
 Firewall
 attaching to WAN 38
 main features 25
 ports 22
 positioning 32
 purpose 22
 quick setup 41
 uses 22
 firewall security 25
 Firewall, moving 41

firmware
 e-mail notification 109
 loading 110
 lost 198
 reloading 199
 uploading 110
 forbidden domains 86
 front panel 34

G

gateway, default 217
 glossary 15

I

IANA 220
 ICMP packets 97
 installation
 inventory 31
 positioning 32
 rack mounting 32
 Installation Wizard 41
 automatic LAN settings 51
 automatic WAN settings 45
 configuring LAN settings 51
 configuring WAN settings 45
 manual WAN settings 45
 setting password 43
 Installation Wizard Welcome Screen 43
 installing
 using the rubber feet 33
 Internet
 filtering 26, 189
 filtering, overview 83
 users 26
 Internet Assigned Numbers Authority 220
 internet filtering 26
 Internet Firewall
 resetting 198
 Internet Relay Chat 16
 Internet Service Provider 16
 InterNIC 217
 intranet settings 140
 IP
 addressing, introduction 215
 defined 215
 port numbers 220
 spoofing 98
 IP address
 classes 216
 defined 16, 216
 Firewall default 42

- sharing 28
- IP Spoof 16
- IRC 16
- ISP 16

J

- Java
 - blocking 97
 - defined 81

K

- keyword
 - field 87

L

- LAN
 - port 22
 - static route settings 144
 - users 26
- LAN settings
 - configuring
 - using Installation Wizard 51
- Land Attack 16
- LED
 - 100 Mbps 34
 - alert 35
 - green 34
 - packet 35
 - power 35
 - self test 35
 - yellow 34
- logs 95
 - and alerts 27
 - buffer 100
 - categories 101
 - deleting contents 100
 - e-mailing 96
 - possible attacks 98
 - probable attacks 98
 - viewing 96

M

- mail server option 99
- main features of Firewall 25
- Management Interface 16
- Management Station 16
 - setting up 42
- manual WAN settings 45
- maximum

- idle time 89
- web usage option 89
- MIBs 248
- moving your Firewall 41

N

- NAT 16, 145
 - overview 28
- network
 - addressing mode 63
- network access rules 26, 119
 - creating 193
 - examples 195
 - hierarchy 194
- Network Address Translation 16
- network configuration
 - diagram 37
- Network News Transfer Protocol 16
- network protocols. *See* protocols
- Network Supervisor, 3Com 23
- network supplier support 248
- Network Time Protocol 16
- networks, introduction 215
- NNTP 16
- notification of new firmware 109
- NTP 16

O

- one-to-one NAT 145
- online technical services 247

P

- packet inspection
 - stateful 25
- Packet LED 35
- Packet Trace tool 77
- password
 - administrator's 200
 - default 200
 - lost 198
 - setting
 - using Installation Wizard 43
 - setting for user authentication 126
- Ping of Death 17
- ping of death 98
- Ping tool 77
- Point-to-Point Portocol over Ethernet 17
- policy rules 119
 - creating 193
- policy, security 25

- port numbers
 - registered 220
 - well-known 220
- ports
 - DMZ 22
 - LAN 22
 - WAN 22
- positioning the Firewall 32
- power adapter socket 36
- power LED 35
- power LED, startup status 38
- power supply
 - redundant 36
- PPPoE 17
- protocols 215
- proxy Web server 138
- public servers, DMZ port 22

Q

- quick setup 41

R

- rack mounting 32
- RADIUS 17
- rear panel 35
- redundant power supply 36
- remote access 28
- remove user, user authentication 127
- reports 103
- reports, displaying 104
- reset option, reports 103
- reset switch 36
- resetting the Internet Firewall 198
- restarting the SuperStack 3 Firewall 105
- restoring
 - configuration 106
 - factory defaults 108
- restricting access
 - to web features 81
- returning products for repair 251
- routes
 - adding 145
 - specifying static 143
- rubber feet 33
- rules, creating 119

S

- safety information 239
- sample network
 - diagram 37

- saving configuration 106
- screen logs, disabling 118
- security functions
 - extending 26
- security policy 25
- self test LED 35
- self-diagnostic tests 38, 200
- services
 - adding 116
 - deleting 118
- setting
 - admin password 60
 - clock 61
 - password
 - using Installation Wizard 43
- setting up a Management Station 42
- settings, reloading 107
- setup, quick 41
- software, upgrading 109
- specifications
 - technical 243
- specified addresses
 - attaching to the LAN 143
 - attaching to the WAN 143
- stateful packet inspection 25
- static routes
 - LAN settings 144
 - specifying 143
- subnet mask
 - defined 217
- SuperStack 3 Firewall
 - restarting 105
- SYN Flood 17
- SYN flood attacks 98
- syslog server 28, 99

T

- TCP packets 97
- TCP/IP, defined 215
- technical
 - specifications 243
 - standards 243
- technical support
 - 3Com Knowledgebase Web Services 247
 - 3Com URL 247
 - network suppliers 248
 - product repair 251
- Technical Support Report 78
- terminology 15
- tests, self-diagnostics 38
- The Learning Company 189
- tools

- diagnostics 76
- DNS Name Lookup 76
- Packet Trace 77
- Ping 77
- top Web site hits 86
- troubleshooting 203
 - Alert LED 204
 - changes not saved 205
 - duplicate IP address errors 205
 - Ethernet connection 204
 - Internet access for LAN users 205
 - Link LED 204
 - log contents 203
 - machines on WAN not reachable 206
 - management interface 204
 - power LED 203, 204
- trusted domains 86

U

- UDP packets 97
- updating users for authentication 126
- upgrading software 109
- uploading firmware 110
- URL 247
 - registration 18
- user
 - privileges 26
 - remote access 28
 - settings, authentication 123
- users
 - advanced 26
 - deleting 127
 - Internet 26
 - LAN 26
- UTC 17

V

- View Log tab 96
- VPN 17

W

- WAN
 - port 22
- WAN settings
 - configuring
 - using Installation Wizard 45
- Web features, restricting 81
- web filtering 26
- web management interface, access lost 198
- web proxy, disabling 82

- Web Site Filter 189
 - activating 192
 - subscription 189
 - updating 83
- Web site hits, reports option 104
- web sites
 - inappropriate 189
 - objectionable, defined 190
- Web Sites to Allow option 86
- Web Sites to Block option 86
- web sites, tracking most accessed 27
- Welcome Screen
 - Installation Wizard 43
- Wizard, Installation 41
- World Wide Web (WWW) 247

REGULATORY NOTICES

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

INFORMATION TO THE USER

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

CSA STATEMENT

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

CE STATEMENT (EUROPE)

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI STATEMENT

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI STATEMENT

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

